Rubrike

Kodiranje - BBC micro:bit

STEM-radionice

Mala škola fotografije

Izbor

Budućnost prijevoznih sredstava

Predivan svijet kristala

Geekcreit UNO R3 starter kit (2)

Praksa ratnih robota

Prilog

Robotski modeli za učenje kroz igru u STEM nastavi – Fischertechnik (72)

ISBN 0400-0315
9 770400 031003

ABC tehnike

www.hztk.hr

ČASOPIS ZA MODELARSTVO I SAMOGRADNJU

Broj 682 | Veljača / February 2025. | Godina LXIX.

Reprezentacija Hrvatskog zrakoplovnog saveza osvojila je treće mjesto - brončanu medalju u ekipnom plasmanu na Svjetskom prvenstvu za radio upravljane jedrilice s elektromotorom u kategoriji FAI F5J, koje je održano od 2. do 8. ožujka 2025. godine, u mjestu Córdoba u Argentini.

Reprezentaciju su činili Arijan Hucaljuk, Saša Pećinar i Nikola Lehkec. Time je ostvaren iznimman rezultat koji pokazuje kontinuitet uspješnih nastupa naših zrakoplovnih modelara na svjetskim natjecanjima, s obzirom na to da je Arijan Hucaljuk već osvajao titulu svjetskog prvaka u pojedinačnoj konkurenciji (za prethodna postignuća nagrađen je i medaljom CIAM Legends Medal koja se dodjeljuje izvanrednim zrakoplovnim modelarima koji su titulu svjetskog prvaka osvojili najmanje tri puta) a reprezentacija je osvojila i srebrnu medalju, odnosno odlično drugo mjesto u ekipnom poretku na Svjetskom prvenstvu 2023. godine. Uz izvanredan rezultat u ekipnom plasmanu hrvatski zrakoplovni modelari ostvarili su zapažen rezultat i u pojedinačnom plasmanu, Nikola Lehkec u ukupnom pojedinačnom poretku osvojio je odlično 5. mjesto.

U OVOM BROJU

Nacrt u prilogu:

Robotski modeli za učenje kroz igru u STEM nastavi – Fischertechnik (72)

Nakladnik: Hrvatska zajednica tehničke kulture, Dalmatinska 12, P. p. 149, 10002 Zagreb, Hrvatska/Croatia

Glavni urednik: Zoran Kušan

Uredništvo: Sanja Kovačević – Društvo pedagoga tehničke kulture Zagreb, Zoran Kušan – urednik, HZTK, Danko Kočiš – ZTK Đakovo

DTP / Layout and design: Zoran Kušan

Lektura i korektura: Morana Kovač

Broj 6 (682), veljača 2025.

Školska godina 2024./2025.

Naslovna stranica: Enigma, umjetnička vizija

Uredništvo i administracija: Dalmatinska 12, P.p. 149, 10002 Zagreb, Hrvatska
telefon (01) 48 48 762 i faks (01) 48 46 979; www.hztk.hr; e-pošta: abc-tehnike@hztk.hr
"ABC tehnike" na adresi www.hztk.hr
Izlazi jedanput na mjesec u školskoj godini (10 brojeva godišnje)
Rukopisi, crteži i fotografije se ne vraćaju
Žiro-račun: Hrvatska zajednica tehničke kulture HR68 2360 0001 1015 5947 0
Devizni račun: Hrvatska zajednica tehničke kulture, Zagreb, Dalmatinska 12, Zagrebačka banka d.d. IBAN: 6823600001101559470 BIC: ZABAHR2X
Tisak: Alfacommerce d.o.o., Zagreb

HRVATSKA ZAJEDNICA TEHNIČKE KULTURE

Ministarstvo znanosti i obrazovanja preporučilo je uporabu "ABC tehnike" u osnovnim i srednjim školama

Budućnost prijevoznih sredstava

Kroz stoljeća, čovječanstvo je napredovalo iz oskudnih početaka, gdje su ljudi jedino mogli putovati pješačenjem ili uz pomoć životinja, u eru modernih prijevoznih sredstava. Prva prekretnica prometa započela je izumom kotača oko 3500 godina prije Krista, što je omogućilo efikasniju mobilnost i početak razvoja transformacije prijevoza. Kasnije, izum i razvoj motora s unutrašnjim izgaranjem dodatno je ubrzao globalnu povezanost te gotovo izbrisao granice i udaljenosti u trgovini i kulturi. Zahvaljujući nizu inovacija u prometu, današnja globalizacija omogućava nam povezanost sa svakim dijelom svijeta. Također brze željeznice, cestovni, zračni i pomorski promet omogućavaju pristup raznovrsnoj robi i proizvodima na globalnom tržištu.

Zašto se prijevozna sredstva mijenjaju?

Prijevozna sredstva danas se neprestano mijenjaju kao odgovor na ekološke, društvene i tehnološke izazove. Iako je njihova proizvodnja bila revolucionarna u poboljšanju mobilnosti, masovna proizvodnja i upotreba dovela je do niza negativnih posljedica. Budući da je ekologija postala glavna tema posljednjih desetljeća, nastoji se dovesti u pitanje razvoj modernih prijevoznih sredstava. Zagađenje zraka, emisije staklenčkih plinova te povećane prometne gužve i buka u gradovima samo su neke od negativnih posljedica koje utječu na zdravlje našeg planeta Zemlje i ljudsku dobrobit. Ekološke posljedice nisu niti kratkotrajne niti bezazlene, već zahtijevaju puno napora, promjena i financijskih sredstava da bi se sanirale. Sredstva transporta pokušavaju se u isto vrijeme modernizirati, a i prilagoditi ekološkim zahtjevima.

Slika 1. Model automobila Detroit Electric coupe iz 1917. godine postizao je brzinu od 40 km/h

Električna vozila

Gotovo svaki peti prodani automobil u 2023. godini na globalnoj razini bio je električni, čime je ukupan broj ove vrste vozila premašio 14 milijuna. Budući da električna vozila (engl. *Electric Vehicle*) (EV) omogućuju znatno smanjenje emisija CO_2, mnoge ekološki osviještene zemlje postavljaju ciljeve za smanjenje emisija plinova te potiču stanovnike na kupnju električnih vozila. Isto su tako već u nekim regijama najavljeni planovi za postupno ukidanje fosilnih goriva u prometu. Među primarnim nedostacima su dugo vrijeme punjenja i kratak vijek trajanja baterije, što se kontinuirano nastoji riješiti novim tehnološkim rješenjima. Jedno od takvih rješenja je proširenje mreže punionica na autocestama i u urbanim sredinama (trenutno dolazi do eksplozivnog rasta u broju javnih punionica) jer bi povećalo praktičnost posjedovanja električnog vozila. Primjerice, do kraja 2022. u svijetu je bilo instalirano oko 2,7 milijuna javnih punjača za EV (uključujući spore i brze punionice), što predstavlja rast od 55% u odnosu na 2021. godinu. Iako Kina prednjači s više od polovice svih punionica, Europa ih ubrzano nadoknađuje. Europska unija je čak donijela propis (engl. *Alternative Fuels Infrastructure Regulation*) kojim članice moraju postaviti punionice svakih 60 km duž glavnih autocesta do kraja desetljeća. Nadalje, gradovi diljem svijeta moderniziraju javni prijevoz kako bi on postao čišći i privlačniji građanima, time smanjujući korištenje osobnih vozila. Veliki su trend električni autobusi koje je Kina već masovno uvela 2020. te tad imala oko 90% svih e-buseva na

Slika 2. Od svih prijevoznih sredstava, kada su u pitanju brzina, kapacitet prijevoza i ekološka održivost, čini se da je željeznica najviše napredovala

Slika 3. Dostava pošiljaka uz pomoć dronova danas se odvija u nekim urbanim i teško dostupnim područjima

svijetu. Ubrzo, elektrifikaciju autobusa provode i Europa i Amerika, te danas prometuje gotovo 600 tisuća električnih autobusa. Dugo najčišći oblik masovnog transporta (jer nemaju lokalnih emisija, a troše struju koja može biti obnovljiva) su električni vlakovi i tramvaji. Naime, još jedna nezanemariva prednost električnih vozila je smanjenje buke u prometnim gradovima zbog toga što ovakva vozila rade gotovo bešumno. Sve ove investicije u električni javni prijevoz smanjuju zagađenje u gradovima i čine prijevoz energetski učinkovitijim.

Znanstvena fantastika ili stvarnost: Robotaksiji i leteći automobili

Slika 4. Električni hiperautomobil Rimac Nevera može dostići brzinu do 412 km/h

Nekima je znanstvena fantastika, a nekima stvarnost, no uistinu roboti se sve više integriraju u naše svakodnevne živote. Robotaksiji (autonomna vozila) koja pomoću umjetne inteligencije zamjenjuju taksiste i pomoću senzora prevoze ljude od točke A do točke B, još uvijek nisu integrirani u hrvatske gradove, no itekako ih možemo pronaći u gradovima poput San Francisca i Los Angelesa, ali i u Kini. Ovakav prijevoz mogao bi smanjiti prometne nesreće, gužve i zastoje. Ipak, prije svega tvrtke moraju osigurati da vozila mogu sigurno raditi u različitim vremenskim uvjetima i prometnim situacijama. Također postoji niz zakonskih prepreka u budućnosti jer većina gradova i zemalja tek treba uspostaviti jasne smjernice za autonomna vozila. Nadalje, koncept letećih automobila koji bi smanjio gužve u prometu i ubrzao prijevoz nam je bliža budućnost. Iako se već zadnjih desetak godina priča o ovoj inovaciji, nedavno je prvi probni "leteći automobil" dobio odobrenje za probne letove. Stoga, ovakvo bi moderno prijevozno sredstvo moglo ubrzo postati naša sadašnjost, koja će mnogo toga promijeniti. Ipak, prije letećih automobila možemo očekivati dronove koji će moći prevoziti robu. Izvorno korišteni za snimanje i dostavu malih paketa, danas se razvijaju električni dronovi s vertikalnim uzlijetanjem i slijetanjem koji mogu prevoziti teret na kratkim i srednjim udaljenostima.

Slika 5. Sve više dostavljačkih službi u uporabu uvodi električna vozila

Hyperloop

Paralelno s cestovnim i zračnim prometom, inovacije se događaju i u željezničkom prijevozu. Razvijaju se brzi vlakovi nove generacije i koncepti poput Hyperloopa za ultrabrzi prijevoz kapsulama kroz vakuumske tunele. Hyperloop predstavlja inovativni koncept brzog transporta koji se odvija unutar vakuumskih cijevi, omogućujući kapsulama da putuju gotovo bez otpora zraka. Ovaj sustav obećava putovanja brzinom koja bi mogla doseći i više od 1000 km/h, čime bi se znatno skratio putnički i teretni transport na velikim udaljenostima. Iako izgradnja ovakvog prijevoznog sredstva nailazi na brojne prepreke poput troškova i mogućnosti izgradnje infrastrukture koja bi omogućila siguran i učinkovit transport na visokim brzinama, kontinuirani tehnološki napredak otvara put ka realizaciji ovog inovativnog koncepta u budućnosti.

Ivo Aščić

Predivan svijet kristala

Kristali, poludrago i drago kamenje fasciniraju nas svojom čarobnošću, unikatnošću i ljepotom još od prapočetaka čovječanstva i oduvijek su bili simboli statusa, povezanosti s božanskim i višim frekvencijama, ljepote i bogatstva. Naš jedinstveni planet Zemlja – univerzalni dragulj sam po sebi – proizvodi čitavu blistavu lepezu anorganskih kemijskih spojeva još od svoga postanka. No, kako oni zapravo nastaju, gdje se sve nalaze i koliko ih susrećemo na domaćem terenu, doznat ćemo u članku koji slijedi!

Na Zemlji je do sada pronađeno i identificirano više od 4000 prirodnih minerala, odnosno anorganskih krutina koje imaju karakterističan kemijski sastav i specifičnu kristalnu strukturu. Sastoje se od jednostavnih molekula ili pojedinačnih elemenata raspoređenih u ponavljajuće lance, molekularne "listove" ili pak trodimenzionalne nizove.

Minerali se obično formiraju kada se rastopljena stijena ili magma ohladi ili pak odvajanjem od vode bogate mineralima, kao što je npr. ona u spiljama. Općenito uzevši, mineralne čestice su male, najčešće formirane u zatvorenim prirodnim "džepovima" kao što su npr. tokovi lave ili prostor između zrnaca sedimenta. Veliki kristali koji se nalaze u geodama i drugim stijenama relativno su rijetki. Geoda je najčešće sferični komad stijene koji ima šupljinu okruženu mineralnim kristalima. Potpuno ispunjene geode, bez šupljine u središtu, nazivaju se nodule i one mogu forimirati kalcedone, tj. mikrokristalinični kvarc poput ahata ili jaspisa. Geode su dakle pravi "lucky find" svakog lovca na kristale, a nastaju taloženjem minerala unutar šupljina u vulkanskim ili sedimentnim stijenama, rupama koje su iskopale životinje, šupljinama koje stvara korijenje drveća i sl. Naime, tijekom vremena, čvrsti sferični oblik šupljine taloženjem silikata iz vode postaje podloga za kristaliziranje minerala pa mineralni kristali rastu u slojevima od rubova geode prema njenoj unutrašnjosti, čime se šupljina konstantno smanjuje. Najčešći minerali koji tvore geodu jesu razni varijeteti kvarca te kalcit. Nikada neću zaboraviti jednu ogromnu

Neobrađeni dijamanti

geodu ametista na koju sam naletjela nekoć davno u jednom alternativnom *shopu* u Veroni... Naravno, jedino što sam si mogla priuštiti jest gledati je i sliniti nad njome jer je cijena takvih stvarčica podjednako impozantna kao i one same, ali... još mi je u sjećanju. Svaka je geoda sama po sebi unikatna kompozicija minerala jer veličina i oblik kristala koje sadrži te njihove različite nijanse čine svaku geodu uistinu posebnom. Pa ipak, gruba i neugledna vanjština geode ne daje ni naslutiti što bi se u njoj moglo nalaziti – to možete otkriti samo ako ju razbijete ili prepilite.

Same su pak stijene napravljene od nakupina ili mješavina minerala, a minerali i stijene utječu na razvoj oblika reljefa baš kao što tvore i prirodne resurse kao što su zlato, kositar, željezo, mramor i granit.

Silikati – uključujući kvarc, tinjac, olivin i dragocjene minerale poput smaragda – najčešća su klasa minerala, kao i glavne komponente većine stijena. Oksidi, sulfidi, sulfati, karbonati i halogenidi druge su pak glavne klase minerala.

Kao što smo već napomenuli, mnogi minerali tvore zaista prekrasne kristale – obično tzv. *poludrago kamenje* – međutim najcjenjeniji među njima su oni koje nazivamo *drago kamenje*. Neobrađeni dragulji pritom često izgledaju prilično obično, pohabano i mutno – više poput običnih kamenčića ili stijena nego li poput kla-

Geoda ametista

sičnog oblika jednog dijamanta! Ja imam jedan maleni neobrađeni rubin za koji biste prije pomislili da je zrno kakva dobrano odstajala tamno crvena graha s lokalnog placa nego li kakav dragi kamen! Doduše, imam i par sitnih plavih safira koji vizualno prije podsjećaju na kakav nusprodukt kokoškina metabolizma no... ipak su safiri s certifikatom! A takve se stvari dobiju za relativno malu paru po mineral u *shopovima* i zalagaonicama. Dakle, shvaćate poantu – tek kada se izrežu i ispoliraju, odnosno obrade, dragulji dobivaju sjaj i ljepotu koja im daje pravu vrijednost. Otuda i onaj izraz da je netko kao "nebrušeni dijamant" (u smislu da ima puno potencijala, ali se to još ne kuži).

Ukratko, povijesno gledano, dragulji se tradicionalno dijele na drago i poludrago kamenje, tj. klasu. Postoji čitav niz predivnog poludragog kamenja, međutim, kao drago kamenje kvalificiraju se samo dijamanti, rubini, safiri i smaragdi. Svojedobno se ametist također smatrao dragim kamenom, ali su kasnije u Brazilu pronađene velike rezerve, što je smanjilo njegovu tržišnu vrijednost. Pritom, navedeno drago kamenje nastaje na različite načine i sastoji se od različitih materijala, što znači da se i njihov izgled uvelike razlikuje. Dijamanti, sastavljeni od atoma ugljika, najtvrđa su prirodna tvar koja se nalazi na Zemlji. Nastali su pod ekstremno visokim tlakom stotinama kilometara pod zemljom, a nalaze se na relativno malo lokacija diljem svijeta. Grafit je također napravljen od atoma ugljika, ali s drugačijim rasporedom – što objašnjava zašto je dijamant najtvrđi mineral, a grafit (koji se koristi u olovci) jedan od najmekših!

Rubini nastaju od minerala koji se naziva *korund*, a sastoji se od aluminijevog oksida. Za njegovu su crvenu boju odgovorni tragovi kroma. Korund također tvori safir u mnogim bojama, koje uglavnom potječu od mješavina željeza, titana i kroma u tragovima.

Smaragdi nastaju od minerala zvanog *beril* čija je kemijska formula složena mješavina berilija, aluminija, silicija i kisika. Boja dolazi od dodatnih tragova kroma i vanadija. Međutim, različiti elementi u tragovima mogu proizvesti druge boje, omogućujući berilu da formira poludrago kamenje poput primjerice akvamarina. Minerali i dragulji su nadalje klasificirani prema svojim fizičkim svojstvima, uključujući tvrdoću, sjaj, boju, gustoću i magnetizam. Također se identificiraju po načinu na koji se lome ili vrsti traga ili pruge koju ostavljaju kada se trljaju o laboratorijski alat koji se naziva *ploča s prugama*. Kristali koje si mi, obični smrtnici u današnje vrijeme najčešće možemo priuštiti i od kojih se uvelike radi nakit koji nosimo obično su oni kvarcni. To su oni općepoznati i vrlo popularni kristali poput npr.

Neobrađeni bijeli kvarc

gorskog kristala (bijeli kvarc) ili ružičastog kvarca (rozenkvarc). No, osim što su lijepi, kvarcni kristali posjeduju i prirodno svojstvo koje se naziva *pietzoelektričnost*, odnosno sposobnost stvaranja električnog polja, što ih čini vrlo korisnim u radio- i videoopremi! Silikonski se pak kristali koriste u proizvodnji čipova koji napajaju naša računala i fotonaponskih stanica koje se koriste u solarnoj tehnologiji. Ipak, vjerojatno najrašireniji uporaba kristala vjerojatno je ona, zbog njihove ljepote već spomenuta – dekorativna. Bilo da se koriste kao dio nakita ili kao ukrasni

predmeti, omiljen su materijal svakome sklonom ukrašavanju. Konačno, kristali zbog svojih specifičnih frekvencija imaju i još jednu podjednako tradicionalo-ritualnu i suvremeno-popularnu primjenu: onu energetsku! Naime, često se koriste kao žarišta za meditaciju, katalizatori za postizanje određenih ciljeva, energetsku zaštitu, samopomoć te iscjeljenje. A ako se pitate možete li i vi, kako i gdje samostalno pronaći kristale u prirodi, vjerujem da i tu možemo pomoći pokojim *hintom*! I zaista, potraga za kristalima jedan je od super načina za provesti dan na otvorenom i uzbudljiva avantura u kojoj nikad ne znate što možete pronaći! Traženje kristala ujedno je i izvrsna prilika da istražite različite krajolike, od planina do riječnih korita te, uz malo sreće, čak i zaista otkrijete zanimljive vrste kristala i predivnog kamenja. No, kako prepoznati prirodni kristal? Prirodni kristali imaju specifične karakteristike koje ih čine jedinstvenima pa svakako obratite pažnju na oblik budući da neki od njih imaju savršeno definirane rubove, dok su drugi nepravilni. Boja i sjaj su im, kako smo već spomenuli, također prilično zagasitiji i neugledniji nego što je to slučaj kod obrađenih primjeraka, no usprkos tome mogu biti nevjerojatno lijepi. Naime, sjaj prirodnih kristala često je suptilan no nepogrešivo prisutan! Štoviše, po mom iskustvu, što je određeni kristal dragocjeniji, u neobrađenoj je formi čak i neugledniji od svojih ekonomski priuštivijih neobrađenih kolega. Tako se, primjerice, cirkon, bezbojni safir ili kristal često prodaju pod krinkom dijamanata. E sad, ako naletite pak na obrađeni kamen, a zanima vas je li pravi, pokušajte kroz njega pogledati u sunce. Kroz pravi brušeni dijamant moguće je vidjeti samo svijetlu točku, dok će lažni dijamant propuštati svjetlost! Nadalje, razlike između prirodnih i obrađenih kristala mogu se prepoznati i po njihovoj teksturi – prirodni kristali često imaju nepravilnosti i sitne nesavršenosti koje doprinose njihovoj autentičnosti. Obrada kristala može uključivati poliranje ili dodavanje boje kako bi izgledali privlačnije, dok pravi ljubitelji kristala vole autentičan izgled, čak i s ponekom nesavršenosti. Također, zapamtite da pitanje kako kristali nastaju u prirodi znatno utječe na njihov konačan izgled – proces kristalizacije može trajati tisućama ili čak milijunima godina, stvarajući strukture koje su fascinantne u svojoj originalnoj formi.

Rubin neobrađeni

Ok, a mogu li se, i koji, kristali naći u Hrvatskoj? Apsolutno! Štoviše, imamo poprilično raznoliku geološku baštinu tako da se i kod nas u prirodi mogu naći brojni kristali i minerali, od kojih podosta njih čak i na Medvednici! Većina naših kristala dolazi iz planinskih područja ili pak starih rudarskih nalazišta, gdje su dugotrajni geološki procesi omogućili njihovo oblikovanje. Neke od najčešćih domaćih vrsta kristala koje možete pronaći su kvarc, ahat, kalcedon, opal, jaspis, aventurin, kalcit, aragonit, fluorit i serpentin.

Kvarc dolazi u različitim oblicima, uključujući gorski/prozirni, ružičasti kvarc te ametist. Gorski kristal čest je na Medvednici i u Gorskom kotaru, dok se ametist može naći u Lici. Kvarc nastaje kad se otopine bogate silicijem hlade ili kad se magmatski procesi događaju duboko ispod Zemljine površine, stvarajući kristale karakterističnog sjaja i strukture.

Ahat se može prepoznati po slojevitim uzorcima i bojama koje variraju od sivih i smeđih do crvenih i plavih nijansi, a njegova nalazišta u Hrvatskoj često su povezana s vulkanskim stijenama i riječnim sedimentima. Prekrasni se primjerci mogu pronaći u okolici Samobora!

Kalcedon se, kao jedan od varijeteta kvarca, odlikuje plavim, sivim i smeđim tonovima te se često pojavljuje u Istri i Dalmaciji. Kristalizacija kalcedona događa se kada se otopine silicijevog dioksida hlade i talože u šupljinama stijena. Zbog svojih nježnih boja i glatke teksture, omiljen je među ljubiteljima minerala.

Opal se kod nas rijetko pronalazi u većim količinama no moguće ga je pronaći na Medvednici i u Istri. Opali su prepoznatljivi po svom irides-

centnom sjaju koji nastaje zbog loma svjetlosti unutar mikroskopskih kuglica silicijevog dioksida. Zbog svoje ljepote i raznolikosti boja, smatra se vrlo dragocjenim kristalom.

Jaspis se pojavljuje u gotovo svim bojama, a može se naći na Banovini i na Medvednici. Jaspis se formira kada se minerali poput željeza talože zajedno sa silicijem, stvarajući slojeve i šare koje kamenu daju jedinstveni izgled.

Aventurin, kamen blagostanja, kvarc je s inkluzijama koje stvaraju metalni sjaj, obično zelene ili plavo-zelene boje, a može se pronaći u Gorskom kotaru. Aventurin nastaje kroz hidrotermalne procese, kada otopine bogate mineralima talože slojeve kvarca s primjesama koje mu daju karakterističan izgled. Gdje konkretno pronaći kristale u prirodi ovisi pak o specifičnim geološkim uvjetima pa je svakako uputno prije ovakve avanture malo istražiti geološku povijest odabranog lokaliteta i, ako ste ikako u prilici, malo se raspitati i među mještanima. Imajte na umu da i procesi poput erozije ili tektonskih pomicanja često otkrivaju nove slojeve bogate kristalima. Naravno, ako odlučite krenuti u takvu potragu za blagom, pritom određenu ulogu igra i sreća pa vam je iz svega srca želimo u izobilju! S druge strane, ako baš i niste skloni takvim avanturama, u ovim sjajnim remek-djelima prirode možete neometano uživati i na nekom od geoloških sajmova, svratiti do kakve specijalizirane trgovine u vašem mjestu ili pak razgledati ponudu kristala *on line*, naći jedan koji zaista rezonira s vama i uživati u njegovoj ljepoti i energiji pored kućnog ognjišta.

Ivana Janković,
Croatian Wildlife Research and Conservation Society

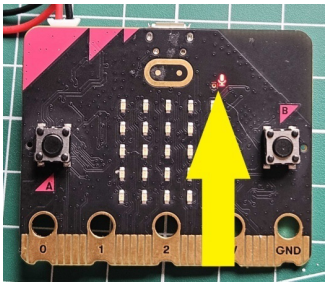
BBC micro:bit [56]

Poštovani čitatelji, nastavljamo seriju kodiranja BBC micro:bita preko jednostavnih primjera u Scratch-Editoru. U ovom ćete nastavku saznati kako iskoristiti neke blokove S-Editora *MicroBit More* koji se tiču osjetila zvuka.

Osjetilo zvuka

Nije to nikakvo posebno osjetilo, to je "najobičniji" mikrofon koji koristimo, na primjer, kod školskog razglasa. Mikrofon je sastavnica koja hvata sve zvučne vibracije koje se proizvode bukom, glasom ili glazbenim instrumentom te ih pretvara u električni napon.

Na pločicu BBC micro:bita v.2. ugrađen je mikrofon koji obnaša funkciju osjetila zvuka, Slika 56.1.

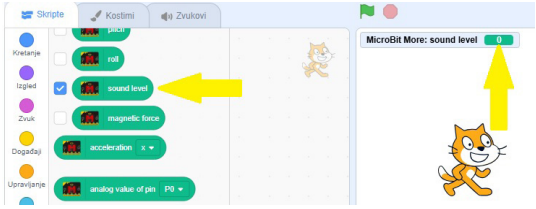


Slika 56.1. Na donju stranu pločice BBC micro:bita v.2. ugrađen je mikrofon. Kako bi zvuk dopro do tog osjetila s gornje strane pločice probušena je rupica. Osjetilo je aktivno kada svijetli crveni simbol mikrofona

Nažalost, na pločici BBC micro:bit v.1. nije predviđeno to osjetilo pa ćete zadatke koji slijede moći izvesti samo ako radite s BBC micro:bitom v.2.

1. zadatak

Neposredno očitavanje jačine zvuka moguće je izvesti kad u izborniku kvačicom označite blok "*sound level*", Slika 56.2.



Slika 56.2. Vrijednosti dobivene s osjetila zvuka moguće je čitati neposredno, bez kodiranja bilo kakvog programa

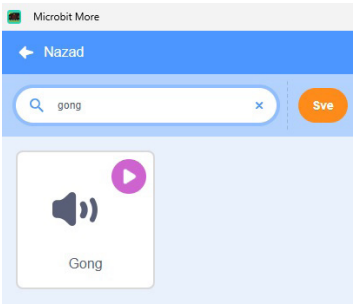
BBC micro:bit uparite sa Scratchom. U blizini mikrofona BBC micro:bita zaplješkite i promatrajte vrijednosti koje se pojavljuju iznad mačke.

2. zadatak

U ovom ćete zadatku proučiti kako se brojevi mijenjaju ovisno o jačini zvuka. Kreće se od tihog

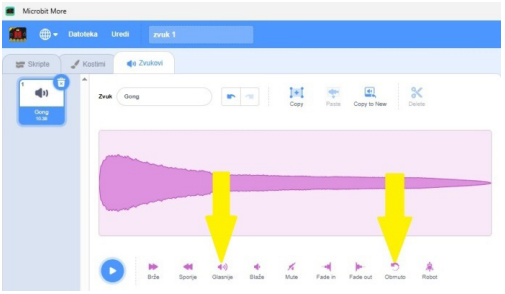
prema jakom zvuku. Za to ćete iskoristiti postojeći zvuk gonga.

Najprije u Scratchu učitajte zvuk gonga. Za to na traci izbornika kliknite na "Zvukovi". Nakon toga kliknite na "Odaberi zvuk", a potom u tražilicu upišite "gong", Slika 56.3.



Slika 56.3. Zvuk gonga

Kliknite po ikoni gonga kako biste zvuk uvezli u program koji stvarate. Otvara se uređivač zvuka s grafičkim prikazom zvuka gonga, Slika 56.4.



Slika 56.4. Grafički prikaz zvuka gonga prikazan u uređivaču zvukova

Pojačajte zvuk, četiri puta zaredom kliknite na programsku tipku "Glasnije". Nadalje, želimo da se zvuk prilikom izvođenja pojačava, a ne stišava pa radi toga kliknite na programsku tipku "Obrnuto". Dobit ćete ono što se traži, Slika 56.5.

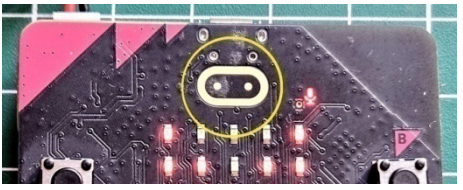
Slika 56.5. Grafički prikaz pojačanog zvuka gonga, od tišeg prema glasnijem

Spremni ste za kodiranje pa se vratite u "Skripte". Prepišite ponuđeni kôd, Slika 56.6.

Slika 56.6. Programski kôd koji će pokrenuti zvuk na zvučnicima računala i koji će pokrenuti mjerenje jačine zvuka preko osjetila BBC micro:bita

Ovdje treba skrenuti pozornost da valja imenovati varijablu, na primjer "jačina zvuka", sve ostalo bi trebalo biti jasno.

Sa Scratchom uparite BBC micro:bit. Pločicu BBC micro:bita približite zvučniku vašeg računala te pokrenite program. Za pokretanje programa kažiprstom dodirnite logo jer to zahtijeva prvi blok programa (*when pin LOGO is touched*), Slika 56.7.



Slika 56.7. Pozlaćeni logo BBC micro:bita

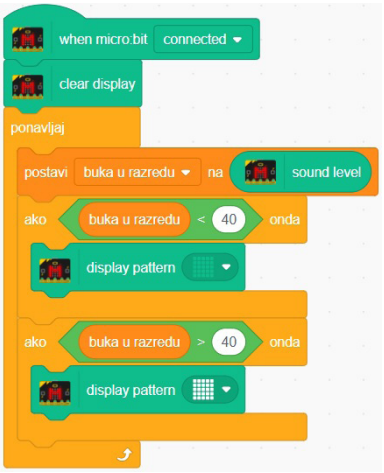
Ako je sve kako valja, iz zvučnika računala čuje se zvuk gonga (u obrnutom slijedu, od tišeg prema glasnijem), a na zaslonu računala u oblaku iznad mačke ispisuju se brojevi koji pokazuju jačinu zvuka.

Ako u prostoriji vlada potpuna tišina, onda se netom nakon startanja programa u oblaku čita 0. Kod najjačeg zvuka vrijednost ide do 51,4.

3. zadatak

Kod ovog zadatka BBC micro:bit mjerit će žamor u vašem razredu. U trenutku kada žamor prijeđe prag i postane buka upalit će se sve LED-ice displeja BBC micro:bita.

Prepišite ponuđeni program sa Slike 56.8.



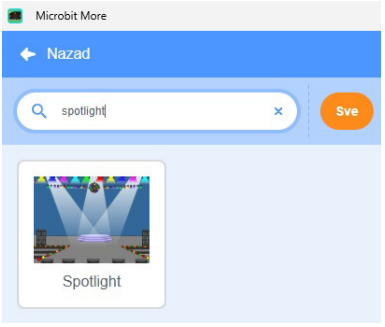
Slika 56.8. Programski kôd za upozoravanje na buku u razredu

Kod određivanja praga (u ovom primjeru upisan je prag 40) zatražite suradnju učenika iz vašeg razreda. Dogovorite se koji bi žamor mogao biti prihvatljiv pa ga isprobajte. Potom, prema dobivenoj jačini zvuka ugodite prag u gornjem programu.

4. zadatak

Jeste li ikad bili u disko-klubu? Igre svjetlosti očaravajuće su, zar ne? Djelomični ugođaj možete ostvariti i na zaslonu računala pa krenite s kodiranjem.

U S-editoru najprije učitajte potrebnu pozadinu. Kliknite na "Odaberi pozadinu" (nalazi se dolje, desno). U tražilicu upišite "*spotlight*", Slika 56.9.

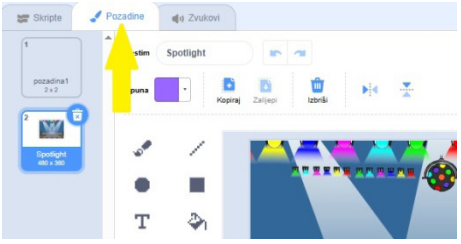


Slika 56.9. Pozadina "*Spotlight*"

Kliknite po ikoni koja se pojavljuje kako biste tu novu pozadinu učitali. Potom u skriptu kliknite na programsku tipku "Pozornica" (nalazi se dolje, desno), tako da poplavi, Slika 56.10.

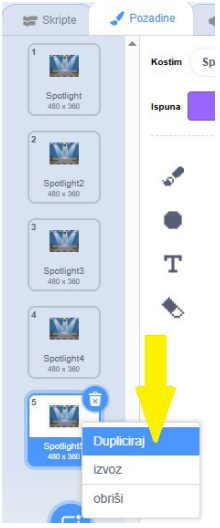
Slika 56.10. Pozornica je aktivna kada je plave boje

Otvorite pozadinu u uređivaču slika, kliknite na programsku tipku "Pozadine", Slika 56.11.



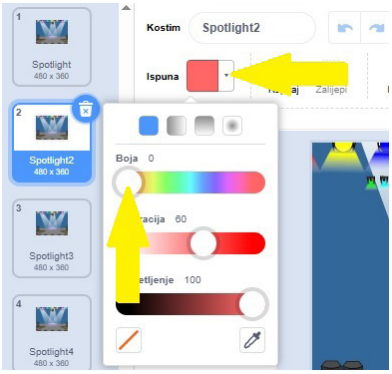
Slika 56.11. Do uređivača slika dolazi se klikom na "Pozadine"

Obilježite ikonu "pozadina1 2 × 2" tako da poplavi pa ju izbrišite klikom po košu za smeće. Ostala vam je ikona "*Spotlight* 480 × 360" koju ćete kopirati četiri puta. Kako? Desni klik na ikonu te u padajućem izborniku izabrati "Dupliciraj" i tako još tri puta, Slika 56.12.



Slika 56.12. U ovom zadatku trebate ukupno pet istih pozadina

Uredite pozadine. Prvu pozadinu preskočite. Obilježite drugu pozadinu tako da poplavi. Kliknite na "Ispuna", a zatim pomaknite klizač boja skroz ulijevo tako da dobijete crvenu boju, Slika 56.13.

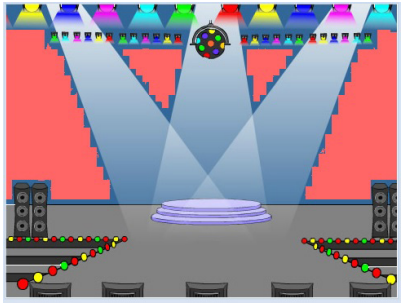


Slika 56.13. Biranje boje

Izaberite alat "Ispuna" tako da kliknete na programsku tipku s nacrtanom posudom boje koja se toči, Slika 56.14.

Slika 56.14. U alatu za bojanje izaberite "Ispuna"

Izabranim alatom na slici pozornice kliknite po svim većim plavim područjima tako da pocrvene, Slika 56.15.

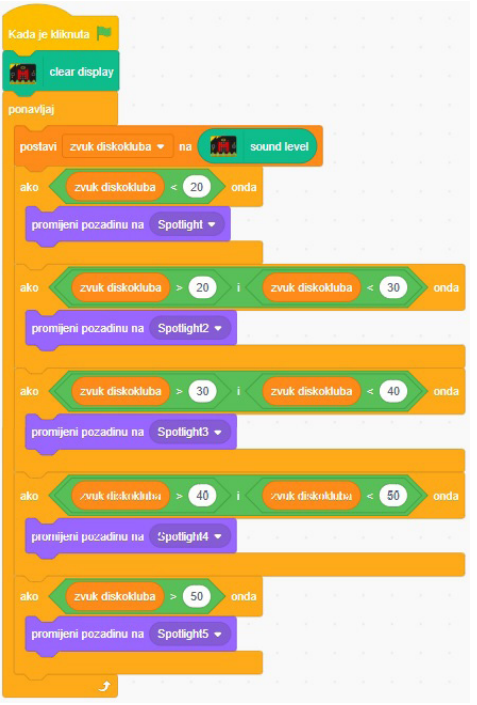


Slika 56.15. Ovako izgleda pozadina2 nakon bojanja u crveno

Obilježite treću pozadinu pa nastavite s opisanim radnjama kako biste pozadinu3 obojali u žuto.

Sve ponovite za četvrtu i petu pozadinu tako da svakoj pridružite drugačiju boju.

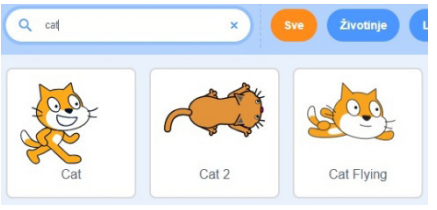
Kad završite sa sređivanjem pozadina vratite se u skript te prepišite ponuđeni program, Slika 56.16.



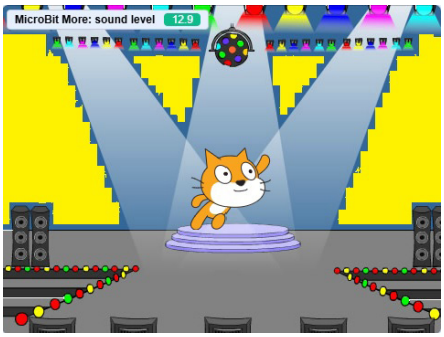
Slika 56.16. Programski kôd igre svjetlosti

Uparite BBC micro:bit te pokrenite program. Na vašem mobitelu pokrenite izvođenje neke pjesme. Pločicu BBC micro:bita približite zvučniku mobitela i promatrajte pozadinu na zaslonu računala. Ako je sve kako valja, boje pozadine mijenjaju se ovisno o trenutnoj jačini zvuka.

Želite li dodatno ukrasiti program onda biste mogli primetnuti razne likove mačke, Slika 56.17.



Slika 56.17. U Scratchu postoje razni likovi mačke (u tražilici upišite *cat*)



Slika 56.18. Mačka pleše u ritmu muzike

U kodu, nakon svakog bloka promjene pozadine, dodajte blokove mačke u raznim pozama. Dobit ćete mačku koja pleše, Slika 56.18.

To bi za sada bilo sve. Vježbajte i uživajte.

Za ove ste vježbe trebali:

- BBC micro:bit v.2.
- USB kabel
- baterije za BBC micro:bit.

Marino Čikeš, prof.

Znanstvenici s Oxforda postigli su teleportaciju pomoću kvantnog superračunala

Ovo će postignuće približiti kvantno računalstvo širokoj praktičnoj upotrebi

Velika prekretnica u kvantnom računalstvu postignuta je nakon što su istraživači sa Sveučilišta u Oxfordu izgradili skalabilno kvantno superračunalo sposobno za kvantnu teleportaciju.

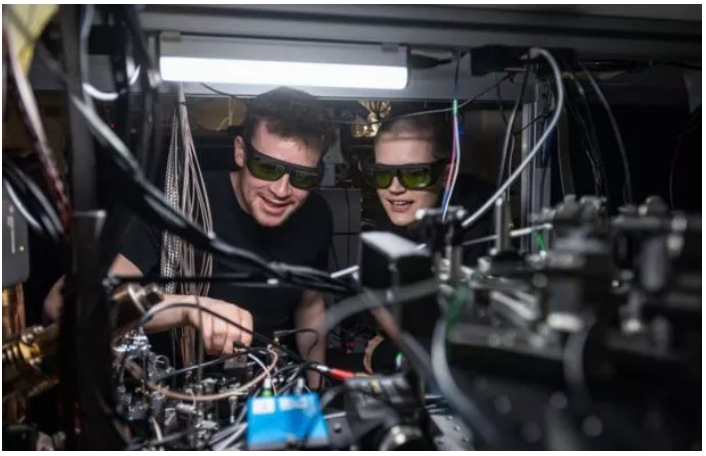
Proboj je usmjeren na takozvani problem skalabilnosti kvantnog računalstva, a istraživači tvrde da će omogućiti realizaciju tehnologije sljedeće generacije na razini koja će poremetiti industriju.

Oxfordski istraživači kažu da kvantna teleportacija koju su postigli postavlja temelje za "kvantni internet"
Izvor: Thred

Područje kvantnog računalstva postoji već desetljećima, ali tek su posljednjih godina napravljeni značajni pomaci u njihovoj realizaciji u praktičnoj mjeri.

Umjesto bitova – kubiti

Koristeći svojstva kvantne fizike, ovi strojevi nove generacije zamjenjuju tradicionalne bitove, jedinice i nule koji se koriste za pohranu i prije-



Dougal Main i Beth Nichol rade na distribuiranom kvantnom računalu
Izvor: John Cairns

nos digitalnih informacija – kvantnim bitovima (kubitima), koji mogu djelovati kao jedinica i nula u isto vrijeme kroz fenomen poznat kao superpozicija.

To kvantnim računalima daje potencijal da budu moćniji od današnjih najsuvremenijih superračunala koja koriste konvencionalnu računalnu tehnologiju.

Ovo nije prvi put da su znanstvenici postigli kvantnu teleportaciju, a timovi su prethodno prenosili podatke s jedne lokacije na drugu bez pomicanja kubita. Međutim, to je prva demonstracija kvantne teleportacije logičkih vrata – minimalnih komponenti algoritma – preko mrežne veze.

Istraživači tvrde da bi tehnika kvantne teleportacije mogla biti temelj za budući "kvantni internet", koji bi nudio ultrasigurnu mrežu za komunikaciju, računanje i senzore.

"Prethodne demonstracije kvantne teleportacije bile su usredotočene na prijenos kvantnih stanja između fizički odvojenih sustava", kaže Dougal Main, s Odsjeka za fiziku na Sveučilištu u Oxfordu, koji je vodio studiju.

Kvantna obrada informacija izvediva trenutnom tehnologijom

"U našoj studiji koristimo kvantnu teleportaciju za stvaranje interakcija između tih udaljenih sustava. Pažljivim prilagođavanjem ovih interakcija možemo izvesti logički kvantni prolaz – temeljne operacije kvantnog računalstva – između kubita smještenih u zasebnim kvantnim računalima.

"Ovo otkriće omogućuje nam učinkovito 'spajanje' različitih kvantnih procesora u jedno, potpuno povezano kvantno računalo."

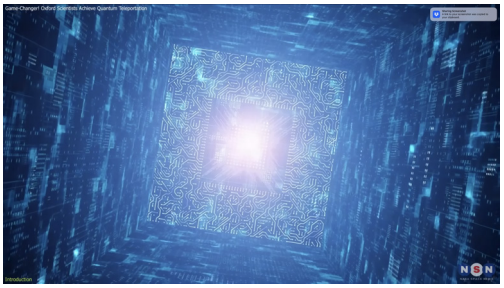
Istraživači su također pokazali da se kvantni sustav može izgraditi i skalirati korištenjem tehnologije koja je već dostupna.

"Naš eksperiment pokazuje da je mrežno distribuirana kvantna obrada informacija izvediva s trenutnom tehnologijom", tvrdi profesor David Lucas, glavni istraživač istraživačkog tima i vodeći znanstvenik u britanskom Quantum Computing and Simulation Hub.

Skaliranje kvantnih računala ostaje ogroman tehnički izazov koji će vjerojatno zahtijevati nove uvide u fiziku, kao i intenzivne inženjerske napore u nadolazećim godinama.

ww.independent.co.uk

Snježana Krčmar



Video
https://www.youtube.com/watch?v=TK48to74q-g&ab_channel=NASASpaceNews

Učimo šifriranje: Klasične metode sigurnosti

U svijetu gdje informacije putuju brže nego ikad, njihova sigurnost postaje ključna. Šifriranje podataka, iako danas visoko sofisticirano, svoje korijene vuče iz jednostavnih, ali genijalnih sustava klasične kriptografije. Jeste li se ikada zapitali kako su tajne poruke prenosili vojnici ili kako su šifre čuvale najvažnije povijesne tajne? U ovom članku istražujemo osnove klasičnog šifriranja i otkrivamo kako supstitucijske i transpozicijske šifre predstavljaju temelj modernih sigurnosnih sustava.

Kada sam bio u osnovnoj školi, kao dijete, pričali smo o šiframa. Pravili smo se važni kako možemo napraviti šifru koju sigurno nitko ne može "provaliti". Takva dječja šifra bazirala se na tome da bi svako slovo neke poruke koju treba šifrirati zamijenili nekim posebnim znakom kojeg bi samo mi znali. Primjerice, umjesto slova A pisali bi simbol naopakog upitnika (¿), za slovo B bi pisali simbol plus-minus (±) i tako dalje. Primjer takve šifre se može vidjeti na slici 1 gdje je prikazana šifrirana poruka sa simbolima.

Supstitucijske šifre: Zamjena slova simbolima i brojevima

Možemo reći da je to šifra koja "obična" slova mijenja simbolima. Riječ zamjena na latinskom se kaže *substitutio* pa se takav sustav šifriranja naziva supstitucijski, a šifra supstitucijska šifra.

Slika 1. Slika šifrirane poštanske karte. Šifra je poznata pod nazivom Pig-Pen

Ako gledamo s praktične strane, teško je pisati takvu šifriranu poruku jer nemamo uvježbane pokrete olovkom kao što to imamo s brojevima i slovima. Samo po sebi se nameće da se umjesto simbola mogu koristiti primjerice brojevi. S brojevima je lako manipulirati. Poput slova, brojevi se mogu zapisivati i na kompjuteru puno lakše nego simboli.

Tako bi slovo A u nekom tekstu supstituirali (zamijenili) za broj 01, slovo B za 02 i slično. Kako bi šifrant jednostavnije šifrirao, pokraj sebe bi morao imati tablicu sa svim slovima i njihovim supstituentima, brojevima. Takva tablica 1 znatno olakšava brzinu šifriranja ako se šifrira olovkom i papirom.

Tablica 1. Prikaz slova i njihovih supstituenata brojeva

A	B	C	D	E	F	G	H	I	J	K	L	M
01	02	03	04	05	06	07	08	09	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Ako bismo htjeli šifrirati poruku koja glasi "ABC TEHNIKE", tada bismo umjesto slova A pisali 01, umjesto slova B pisali 02 i tako za sva slova. Dobivena šifra bila bi zapisana kako slijedi:

01020 32005 08140 91105

Radi preglednosti ali i sigurnosti, brojeve odvajamo u grupe, primjerice od 5 ili 4 slova u bloku. Može se koristiti i neki drugi broj slova u bloku. Kod šifranata tijekom Drugog svjetskog rata, Nijemci su blokove često formirali sa 4 slova, a saveznici s 5 slova u bloku.

Osoba koja primi šifriranu poruku, ako ima tablicu, može vratiti šifriranu poruku nazad u prvobitni tekst. To se radi tako da se postupi obrnutim redoslijedom. Čitaju se brojevi po dvije znamenke i uz pomoć tablice 1 čitaju se slova. Tako će 01 predstavljati slovo A, 02 slovo B i slično.

Takva šifra je, naravno, laka meta bilo kome tko se imalo razumije u šifriranje. Dovoljno je da osoba koja razbija šifru shvati da se radi o supstituciji i intuitivno će zaključiti da bi redoslijed slova u abecedi zapravo bio broj u šifri. U tom slučaju šifra je "provaljena". Osoba koja je provalila tu šifru sada može pročitati sve poruke koje ima i koje su šifrirane takvim sustavom. Šteta može biti ogromna jer su sve poruke pisane tom šifrom razotkrivene. Osim

toga, takva se šifra ne bi mogla koristiti za veći broj ljudi koji bi je primjenjivali. Zamislimo da vojska primjenjuje takvu šifru. Ako bi neprijatelj zarobio samo jednog vojnika koji bi rekao kako ta šifra "radi", tada bi neprijatelj mogao pročitati sve poruke koje ima kod sebe.

Ključ u šifriranju: Dodavanje dodatne sigurnosti

Kako bi nadišli takve probleme, potrebno je u šifru unijeti ključ. Ključ ima ulogu da se neka šifra "zaključa", pošalje do osobe koja je "otključa" istim ključem. Sve one osobe koje nemaju ključ, u osnovi, ne mogu pročitati šifriranu poruku. To bi značilo da ako neprijatelj uhvati vojnika s ključem, on će ukrasti njegov ključ i tim će ključem pročitati samo one šifre koje su šifrirane tim ključem, a druge ne. To je samo jedan od razloga zašto je potrebno što češće mijenjati ključ.

Prije nego što objasnimo kako ključ funkcionira, potrebno je upoznati se s osnovama šifriranja.

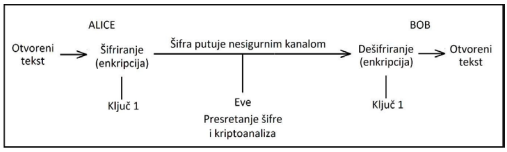
Postupak šifriranja zove se enkripcija, a to znači da se običan tekst prevodi u šifrirani. U našem primjeru, šifriranje ili enkripcija odvijala se supstitucijom slova za broj. Postupak u kojem se šifrirani tekst prevodi natrag u otvoreni tekst zove se dekripcija ili dešifriranje, a vrši je osoba kojoj je ta poruka namijenjena. Osoba koja hvata šifriranu poruku, odnosno presreće je, njoj šifrirana poruka nije namijenjena, a ona tu poruku pokušava razbiti ili vrši kriptoanalizu nad tom porukom.

Osoba koja šifrira i šalje poruku najčešće se označava imenom Alice, osoba koja je prima je Bob i njoj je poruka namijenjena, a Eve je osoba koja presreće poruku i pokušava je odgonetnuti. Dakle, Alice je šifrer i vrši enkripciju, Bob je dešifrer i vrši dekripciju, a Eve je kriptoanalitičar koji pokušava razbiti šifru. Alice i Bob imaju ključ, a Eve nema ključ i ona pokušava pročitati šifrirani ili kriptirani tekst tako da primjenjuje razne napade na šifru.

Također je potrebno nešto reći i o tekstu koji Alice šifrira. Tekst koji želimo šifrirati naziva se otvoreni tekst, a kada ga jednom zašifriramo, naziva se šifrirani tekst.

Sada se vratimo na tablicu 1. Gornji red u tablici predstavlja slova, a donji red su brojevi. Gornji red je otvoreni alfabet, a donji red je šifrirani alfabet. Otvoreni tekst sadrži slova otvorenog alfabeta, a šifrat sadrži slova, brojeve, simbole šifriranog alfabeta.

Kako bi to sve lakše sumirali, prikazana je slika 2. Alice ima otvoreni tekst i želi ga nesigurnim kanalom poslati Bobu. Zamislimo da se Alice nalazi u kući gdje šifrira poruku i šalje je do druge kuće gdje se nalazi Bob. Poruku šalje nesigurnim kanalom, a to može biti, primjerice, telefonska žica koja spaja te dvije kuće, radiovalovima, zvučnim signalima, svjetlosnim i slično. Negdje između, na pola puta gdje se nalaze te dvije kuće, nalazi se Eve. Ona se nalazi u nekoj prislušnoj stanici gdje prikuplja bilo električne signale, sluša radiopromet na točnoj frekvenciji ili na bilo koji način prikuplja informacije koje se šalju iz jedne u drugu kuću. Alice i Bob žele tajno komunicirati i radi toga jedino njih dvoje smiju razmjenjivati informacije. Kako bi to uspjeli, moraju šifrirati svoje poruke i slati ih nesigurnim kanalom. Nesigurni kanal je zajedničko mjesto na koje Alice, Bob i Eve imaju "pristup".



Slika 2. Prikaz postupka šifriranja, dešifriranja i kriptoanalize

Sam postupak šifriranja provodi se tako da Alice uz pomoć ključa i dogovorenog sustava za šifriranje šifrira otvoreni tekst. Dobivena šifra šalje se nesigurnim kanalom do Boba, koji uz pomoć tog istog ključa šifru dešifrira i dobiva otvoreni tekst koji je pogodan za čitanje. Eve je presrela šifru i nad njom vrši kriptoanalizu. Primijetimo, Eve nema ključ. Ona mora poznavati tehnike i alate kriptoanalize kako bi probila poruku.

Simetrično šifriranje: Dijeljenje tajni

Takav sustav šifriranja naziva se simetrični sustav šifriranja. Simetrični sustav se zove tako zato što se koristi isti ključ za šifriranje i dešifriranje. Nedostatak tog sustava je taj što Alice i Bob moraju imati isti ključ. To bi značilo da Alice i Bob moraju izaći iz kuće i na siguran način razmijeniti ključeve. Tu radnju moraju izvesti tako da Eve ne sazna za njihove ključeve. Nakon što su Alice i Bob razmijenili ključeve, sada se mogu dopisivati. Hoće li se sigurno dopisivati, ovisi o jačini kriptosustava koji koristi za kriptiranje i sposobnosti Eve kao kriptoanalitičara, te o čestim izmjenama ključeva i slično.

Iz opisanog primjera može se pogrešno zaključiti da je izmjena ključa u praksi jednostavna.

Primjerice, tijekom Drugog svjetskog rata, brodovi su imali tajnu knjigu ključeva koju su koristili. Kada bi se svi ključevi "potrošili", jer se oni često moraju mijenjati zbog sigurnosti, tada bi posada broda, kao i svi brodovi koji bi htjeli tajno komunicirati, morali pribaviti i razdijeliti knjigu s tajnim ključevima. Također, ako bi špijun ukrao knjigu s ključevima, komunikacija bi se ugrozila; u tom trenutku bi svi brodovi morali dobiti nove knjige s ključevima. To nije jednostavan postupak s obzirom na to da te knjige s ključevima treba dostaviti na daleka mjesta. Sama dostava knjiga rizičan je posao jer se knjige mogu ukrasti. Takve knjige tijekom Drugog svjetskog rata bile su s olovnim koricama kako bi, u slučaju potapanja broda, one potonule i tako se osiguralo da ne dođu u ruke neprijatelju.

Takvi nedostaci doveli su do toga da se danas koriste kriptosustavi s javnim, a ne simetričnim ključevima. Javni ključ nije tema ovog članka pa ćemo se vratiti na naš sustav sa simetričnim ključem. Razmotrimo sada šifrirani alfabet koji koristi Alice, on je prikazan u tablici 1. Kako se u taj supstitucijski kriptosustav može "ugraditi" ključ i kakav on ima utjecaj na šifriranu poruku?

Uzimo isti otvoreni tekst koji Alice treba šifrirati: ABC TEHNIKE. Kriptosustav koji bi koristili je supstitucija koju ja nazivam slovo za broj, a njen postupak provodi se kako smo već vidjeli. Sada promotrimo kako se primjenjuje ključ u tom sustavu i koja je njena sigurnost. Neka ključ bude broj 01251910. Na temelju takvog ključa definira se šifrirani alfabet, tablica 2.

Tablica 2. Prikaz slova u alfabetu otvorenog teksta i ključa u šifriranom alfabetu za supstitucijsku šifru slovo u broj

A	B	C	D	E	F	G	H	I	J	K	L	M
01	25	1G	10	02	03	04	05	06	07	08	09	11
Ključ												

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
12	13	14	15	16	17	18	20	21	22	23	24	26

Kako smo primijenili ključ? Kako smo rekli, tablica za supstituciju sastoji se od otvorenog alfabeta, to su slova u tablici koja se odnose na otvoreni tekst, šifrirani alfabet su u ovom slučaju brojevi koji se nalaze u šifri, a tablica prikazuje pravilo supstitucije. Ključ je taj koji definira šifrirani alfabet. Šifrirani alfabet može se kreirati i na druge načine, ali ovaj je pogodan kako bi se jasno prikazala primjena ključa.

Ključ smo proizvoljno odabrali. Te proizvoljne brojeve prve upisujemo slijeva nadesno u šifrirani alfabet, a ostale brojeve unosimo u niz tako da već korištene brojeve ne unosimo ponovno. Zbog toga je u nizu pojedini broj, koji smo unijeli na početku, a koji je bio dio ključa, izostavljen.

Prema novoj tablici sada šifriramo poruku "ABC TEHNIKE" i dobivamo sljedeći šifrirani tekst:

01251 91802 05120 60802

Sada vidimo ulogu ključa. Isti otvoreni tekst, ali različit šifrirani tekst. Takvu poruku Alice šalje Bobu, a presreće je Eve.

Što Bob radi? On ima tajni ključ (01251910) i na temelju njega formira tablicu 2 po istom pravilu kako ne bi bilo pogreške u dešifriranju.

Bob očitava prva dva broja u primljenoj šifriranoj poruci. Tako će prema formiranoj tablici 2 za 01 očitati slovo A, za 25 očitati B i tako dalje dok se ne dobije otvoreni tekst ABC TEHNIKE.

Eve, koja je presrela njihovu poruku, sada pokušava prema staroj tablici 1 dobiti tekst. Zamislimo da je Eve uspjela špijunažom saznati kako tablica 1 izgleda. Na temelju toga brzo je zaključila da se radi o supstituciji i pročitala stare šifrirane poruke. Sad kada su Alice i Bob uveli sustav ključa u svoj sustav šifriranja, to bitno otežava Evi da pročita novu šifru jer ne zna kako su brojevi raspoređeni u šifriranom alfabetu. Ovdje je bitno napomenuti, a što je ujedno i teško razumjeti kod početnika koji se bave kriptografijom, da se tajnom mora držati jedino ključ, a ne sami princip šifriranja. Kako ovaj primjer i pokazuje, Eva zna kako se postupak šifriranja i dešifriranja provodi, zna da je to jednostavna supstitucija i lako se primjenjuje, jer je to saznala špijunažom. Međutim, to joj ne daje nikakvu mogućnost da pročita šifru ako ne zna njen ključ koji se koristio za šifriranje. Tijekom povijesti je bilo mnogo primjera gdje su se šifre temeljile na tajnosti samog sustava. Tajiti sustav neke šifre je besmisleno. Sjetimo se priče o Enigmi, stroju za šifriranje njemačkih poruka. Koliko god su taj stroj čuvali, saveznici su ipak došli do nje. U tom trenutku saveznici nisu niti jednu poruku uspjeli otkriti jer nisu posjedovali ključ koji je bio primijenjen.

Možete se i sami u to uvjeriti. Objasnite prijatelju kako šifra Slovo za broj funkcionira i neka proba dešifrirati vašu poruku. Sada promijenite ključ i pokušajte mu poslati istu poruku ili neku drugu kako ne bi uspio odgonetnuti bez ključa.

Pravilo koje kaže da samo ključ mora biti tajan, dok sustav za šifriranje može biti javan, naziva se

Nastavak na 24. stranici

MALA ŠKOLA FOTOGRAFIJE

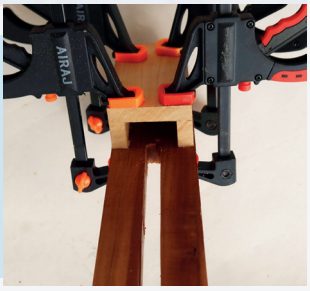
Piše: Borislav Božić, prof.

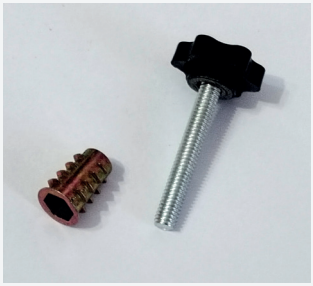
RIJEČANKA 1
peti dio – stativ

S obzirom na veličinu Riječanke 1, na njene gabarite, potreban je stativ tronožac kako bi se njome moglo raditi. Da bi sve bilo u retrostilu, evo postupka izrade stativa. Moguće ga je napraviti u nekoliko varijanti, a ja sam se odlučio na sklopivi tronožac. Osim ovakvog tipa postoje i studijski ili stacionarni stativi. Tronožac je pogodan za terensko snimanje, što i jest namjena ove kamere.

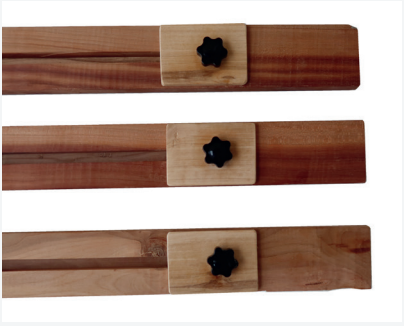
Moguće je konstruirati dva tipa tronošca – jedan s fiksnim nogarima, koji se ne mogu produžavati i koji uvijek imaju istu visinu. Drugi tip tronošca napravljen je tako da na svakom nogaru postoji pomični dio pa se visina može mijenjati. Važan je i dosjed kamere na tronožac. On može biti fiksan, što znači da kameru ne možemo zakretati lijevo-desno, već moramo pomicati cijeli tronožac. Drugi tip dosjeda kamere na tronožac je pokretna "glava" tronošca što prema potrebi omogućuje nesmetano zakretanje i lijevo i desno. Mora se voditi računa i o debljini letvica kako bi mogle izdržati težinu i rad s ovako velikom kamerom. Tronožac treba konstruktivno izvesti tako da pomični dijelovi klize lagano i da se brzo i bez teškoća mogu pomicati. Za to je potrebno precizno mjerenje i obrada sastavnih dijelova.

Gornja slika prikazuje tri osnovne daščice koje su prorezane po sredini. Napravljen je utor po kojem će kliziti vijak koji je učvršćen za unutarnju letvu. Ove su letve od drva šljive. Drvo voćaka dosta je gusto i tvrdo, te je potrebno koristiti oštar alat i uložiti poseban napor kako bi obrada bila precizna. Na ove sam elemente s unutrašnje strane donjeg dijela učvrstio kanal vodilicu za unutrašnju letvu kako to prikazuje slika desno.





Unutrašnja pomična letvica tronošca ima samo ugrađenu maticu u koju se uvrće vijak i njime se regulira pomicanje letvice, tj. visina tronošca. Slika u sredini gore prikazuje tu posebnu ugradnu maticu i vijak s plastičnom glavom kako bi se njime što lakše manipuliralo, odnosno odvrtalo i zavrtalo. Slika desno gore prikazuje pločicu, vodilicu koja se montira s prednje strane osnovne letve tronošca. Pločica na sebi s unutrašnje strane ima učvršćenu malu letvicu koja ulazi u utor osnovne letve i omogućava pravilno vođenje i klizanje unutarnje letve po visini. Vijak prolazi kroz otvor pločice i utor osnovne letve i uvrće se u ugrađenu maticu unutarnje letve. Vrlo se lako i brzo zavrće i odvrće i time se podešava visina tronošca. Na slici desno prikazane su montirane pločice s vijkom na osnovnu letvu.



Gornja i donja slika prikazuju noge tronošca u punoj dužini. Vidljive su pločice i vijci u gornjem dijelu, a u donjem je vodilica unutrašnje letve. Donja slika prikazuje bočnu stranu nogara na kojoj se vidi konstrukcija, tj. odnos vanjske i unutrašnje letve. Vidljivo je da su neki elementi svjetliji, a neki tamniji. Razlog tome je što sam koristio svjetlije drvo trešnje i tamnije, crvenije drvo šljive. Osim vijaka i matica, sve sam dijelove spajao drvenim čepovima i ljepilom kako bih izbjegao upotrebu metalnih spojnih vijaka.

Element koji povezuje tri noge, i time čini tronožac funkcionalnim, napravio sam od šperploče. U središnjem dijelu ovog elementa izbušio sam otvor kako bi u njega sjeo okrugli element učvršćen na donjem dijelu Riječanke 1. Taj okrugli element omogućava kameri zakretanje lijevo i desno, a da se ne pomiče stativ.

Ovaj uski dugački element učvršćuje se s donje strane kamere kako prikazuje slika desno. Služi da bi se kamera učvrstila za tronožac. Okrugli element naliježe u otvor na glavi tronošca i učvršćuje se vijkom s donje strane. Popuštanjem vijka, kamera se po potrebi rotira lijevo ili desno. Element u obliku slova "T" je ekstenzija koja se može izvlačiti za presnimavanje negativa. Kako je to montirano na Riječanki 1, vidljivo je na gornjoj slici.

Ove dvije slike (lijevo od ovoga teksta) prikazuju kako izgleda gotov tronožac i na njega montirana Riječanka 1. Od zamisli, konstrukcije i izrade dug je put. Iako sam za sve napravio skice, nacrte, pripremio materijale, ipak je kod izrade ili isprobavanja funkcionalnosti pojedinih dijelova dolazilo do promjena, do prilagođavanja. Odstupao sam od početne ideje i tražio povoljnija i tehnički jednostavnija rješenja. U konačnici sve je funkcionalno i podređeno osnovnoj ideji pravljenja analognih fotografija.

ANALIZA FOTOGRAFIJA

Cecilija Wollner

1878. – 1942.

Devetnaesto stoljeće je vrijeme sveopćeg civilizacijskog napretka. Industrijalizacija je iznjedrila nove društvene klase, nova zanimanja, nove odnose u društvu, ali je još uvijek zadržan snažan patrijarhalni odnos. Napredak i uspjeh uglavnom su bili rezervirani za mušku populaciju, dok su žene, iako u znatno manjem postotku, ponekad imale priliku graditi karijeru kao umjetnice ili poslovne žene.

Cecilija Wollner jedna je od rijetkih žena fotografkinja i uspješnih žena XIX. stoljeća u Hrvatskoj. Rođena je u fotografskoj obitelji i uz oca je učila zanat. Kao vrlo radoznalo i kreativno dijete brzo je svladavala sve zakonitosti fotografskog zanata – od fotografiranja do laboratorijskog rada. Imućni otac šalje je na školovanje u Beč kako bi što bolje upoznala svijet fotografije u europskoj prijestolnici kulture. Nakon povratka sa školovanja, puna radnog elana i samopouzdanja otvara fotografski atelje 1899. godine pod nazivom Atelier Wollner u Požegi. U svom novom prostranom fotografskom prostoru snima portrete, grupe ljudi, ali izlazi i na teren i pravi prekrasne panorame Požege. Atelje je bio poznat i po tome što je izdavala serije razglednica s motivima Požege i njene okoline. U Požegi je radio još jedan fotografski atelje, Atelier Davidson, s kojim se Cecilija udružuje. Ustvari, udaje se za vlasnika i udruženi ateljei djeluju pod istim imenom Atelier Wolner. U ateljeu su imali nekoliko kamera velikog formata 18 x 24 i 13 x 18 cm s kojima su često išli na teren. Bogata je ostavština ove izvanredne fotografkinje. Njezin opsežan fotografski arhiv, koji je stvorila tijekom svog života, nezaobilazan je za povijest hrvatske fotografije. Gradski muzej Požege čuva arhivu svoje sugrađanke, iz čije su fototeke potekle i fotografije koje objavljujemo u ovom prilogu. Nažalost, stradala je kao žrtva ustaškog režima.

Honey Hilger prešla je dlanom preko malog zaslona i začula kako iza vrata zvoni. Otključavanje. Vrata je otvorila ljudska prilika, srebrnaste vanjštine, bez lica, tek s dva oka na elipsoidu što je bio glava. Leće kamera zastale su na Honey, kao da se pokušavaju sjetiti tko je to pred vratima, a onda se batlerka odmakne u stranu i pokaže joj da uđe.

Honey je svukla kaput i predala ga batlerki da ga objesi na kuku. Osvrnula se po predvorju. Bilo je veliko i prilično mračno. Dva stubišta penjala su se u tamu gornjeg kata. Vrata su bila označena LED svjetlima elektronskih brava. Iz mraka su je promatrale brojne oči uglavljene u kamene kipove, jedne uzvišene, druge zamišljene, neke groteskno iskrivljene do čudovišnosti ili spokojne poput nekoga tko zna sva znanja svemira. Drevni idoli, demoni i bogovi umrlih ili ubijenih civilizacija.

"Gospodin Witt Vas očekuje, gospođice Hilger. Pođite za mnom, molim Vas."

Batlerka ju je povela prema dvostrukim vratima na drugoj strani predvorja. Čuvale su ih dvije zvijeri od kamena, isklesane grubim udarcima čekića i dlijeta. Kipovi su se činili nedovršenima. Ili je njihova nedorađenost prenosila surovu snagu živih zvijeri. Ili… Honey odmahne glavom, nije željela o tome razmišljati.

Vrata su se širom otvorila i srebrna ruka pokaže Honey neka uđe. U skoro potpunom mraku nazirao se obris stola oko kojeg je netko sjedio. Ona nesigurno uđe, a za leđima začuje zvuk zatvaranja vrata.

Nad stolom se polako razgorjelo svjetlo. Kao da je počivalo u zraku, Honey nije mogla vidjeti visi li ili stoji. Oko stola sjedilo je sedam osoba, dlanova položenih na okruglu drvenu plohu. Svi su imali lica pod maskama. Jedna stolica bila je prazna.

"Sjedite, doktorice Hilger", pozvao ju je krupni čovjek nasuprot praznoj stolici.

"Gospodin Witt?" Krupni čovjek kimnuo je glavom. Iza njega stajala je mlada žena u crnom poslovnom odijelu, plave kose strogo složene u punđu, također s maskom na licu.

Honey je sjela. Svi ostali – pet muškaraca i dvije žene – bili su u godinama. Sijede kose, držanje što je otkrivalo duge živote. Ruke su im bile u bijelim rukavicama. Honey se osjećala kao da prisustvuje kakvom sastanku ili obredu tajnog društva.

I nije bila oduševljena time. Drevna arheologija bila je dovoljno zaguljena i bez mračnih rituala i sekti.

"Zašto ste me pozvali?", pitala je Honey nakon desetak sekundi tišine.

"Zbog Vaše stručnosti", odgovorio je Witt. Ostali su je promatrali poput ptica grabljivica, ali nisu ništa rekli. "I sklonosti da radite sama. I za odgovarajuću naknadu. Ovo nije nešto o čemu bi trebalo pričati naokolo, razumijete me?"

Honey kimne glavom.

"Barbara, molim Vas."

Mlada žena izgubi se u tami, a onda se vrati, noseći kutiju prekrivenu tamno zelenom tkaninom. Prišla je Honey i položila je kutiju pred nju. Stala joj je iza leđa.

Honey to nije voljela, ali zaključila je kako molba ili ljutnja neće tu ništa promijeniti.

"Želimo Vaše cijenjeno mišljenje o ovome." Witt pokaže Honey neka razotkrije kutiju. Podigla je tkaninu, uredno je presavinula i položila na stol. Sve to pod netremičnim pogledima zagonetne sedmorke.

Bacila je letimičan pogled na kutiju i simbole urezane u nju. Udahnula je, izdahnula s osjećajem studeni što joj je prešao leđima.

"Želite mišljenje iskusne doktorice arheologije?" Pogledala je ženu iza sebe. "Gospođice Barbara, molim Vas, ako biste bili tako ljubazni da negdje nađete neku sjekiru, rascopate ovo u komadiće, pa da svi zaboravimo da smo to uopće vidjeli."

* * *

"Bojim se da to nije opcija", odvrati Witt. Honey je napravila domaću zadaću o svom domaćinu. Plivao je, metaforički rečeno, u olimpijskom bazenu do ruba punom krupnih novčanica. I bio je strastan, iako vrlo tajnovit proučavatelj arheologije i starina. Ostali oko stola sigurno su imali sličnu strast, inače ne bi bili ovdje.

"Da se ne igramo, gospodine Witt: Vi vrlo dobro znate što je ovo."

"Znam. I znam da je to jedna od tri takve kutije."

"Tri koje su nađene."

"A znam i da ste već otvorili jednu. Pri iskapanju ruševina palače cara Monka XIV."

"Bila sam prisutna. Nisam je ja otvarala."

"Ali ste sigurno zapamtili kako se to radi."

"Jesam. A zapamtila sam i što je bilo poslije."

"To je naš problem. Vaše je da nam otvorite kutiju."

Nad stol se spustila napeta tišina. Honey je dobro znala prijetnju što je dolazila iz kutije. Ono što je bilo unutra nije se smjelo pustiti van. Zapitala se otkud Wittu kutija? I kako zna toliko o njoj?

Galaksija je ogromna. I u njoj je nicalo, cvjetalo i venulo mnoštvo civilizacija. A neke su za sobom ostavile opasna znanja i tehniku. Pa se kroz desetljeća stvorila u arheološkim krugovima prava kabala, koja je – ukratko – određivala što smije u javnost, a što ne. Doktorica Hilger bila je u tom povlaštenom krugu. I bila je svjesna što je to pred njom i koliko je opasno.

"Ne", odgovorila je konačno.

Tišina.

"Recite, doktorice, koliko Vam prstiju treba za otvoriti ovu kutiju?", pitala je jedna od dviju žena za stolom. Honey se nije dopao njen ton.

"Ne razumijem..."

"Deset? Ili Vam je možda dovoljno devet? Ili osam? Sedam?"

Honey pogleda Barbaru. Držala je sklopljeni nož. Honey nije sumnjala da je sječivo dovoljno oštro za odrezati prst.

"Imamo načina da Vas prisilimo, doktorice. Nemojte nas tjerati da im pribjegnemo", zaprijetio je Witt tiho. Honey nije znala koliko je znao o njoj, koliko se raspitivao, ali nešto mu je očito promaklo: nije voljela da joj se prijeti.

"Dobro", podigla je ruke u zrak. "Vaš pogreb. Ali prvo, da vidim novac!"

* * *

Muškarac desno od Witta postavio je tri kamere u polukrug oko Honey. Zatvorila je oči, prizivala pokrete rukama i prstima potrebne da se otvori kutija. U potpunoj tišini, prionula je poslu. Okretala je dijelove kutije, poravnavala simbole, rješavala drevnu zagonetku, koju zapravo nikad nisu do kraja razumjeli. Znala je da je kutija portal. Vidjela je i što može proći kroz njega. Kuda je portal vodio, nije znala. Sedmero za stolom to kao da nije zanimalo. Svjesna tek tri crvene diode na kamerama, osjećala je kako joj kroz prste bride vibracije i razlijevaju se kroz šake i dalje, u ruke. Još dva simbola za poravnati i onda...

Začuo se škljocaj iz kutije. Honey se odmakla od stola. Povukla je za sobom i kovčeg s novcem. Svi u prostoriji osim nje bili su već mrtvi. Ali sami su rekli kako je to njihov problem. Ona možda uhvati kritične sekunde i pobjegne. Nije trebala otvoriti kutiju. Ali, prsti su joj bili dragi. A i novac uvijek dobro dođe.

Honey baci pogled na Barbaru. Stajala je napeto, zureći u kutiju.

Rastvorena kutija počivala je možda minutu na stolu.

A onda ih je sve obasjao snažan bljesak. Svjetlo je nahrupilo u prostoriju, kao da je netko strgnuo stare, trule zavjese s prozora. Barbara je zaklonila oči dlanom.

Iz kutije se uvis izvio krak. Imao je redove nazubljenih prianjaljki. Završavao je u zubatim čeljustima, dovoljno velikim da od tijela otkinu povelike komade mesa. Sa zuba je kapala slina. Krak je izlazio iz nečeg što bi inače podsjećalo na napuhnuto, izvitopereno tijelo kakvog kerubina bez krila. I udovi su bili slični, ali izlomljenih prstiju što su završavali oštrim noktima. Honey je postala svjesna tihog mrmljanja s druge strane stola. Znala je što sedmorka radi. Prizvali su stvora i sad su se nadali obuzdati ga i podvrći svojoj volji.

Odjednom, čudovište je okrenulo svoja smrdljiva usta prema Honey. Barbara je tiho kriknula, ali stvor ju je ignorirao. Usta su visjela na kraku i prilazila sve bliže doktorici.

"Je li ovo isti stvor kao i prije?", pitao je Witt.

"Da", jedva čujno je odgovorila Honey.

"Ima nešto što sam siguran da ne znate o njemu."

"A što to?" Honey je osjećala kako je obuhvaća neka nejasna tromost, kako joj glava hoće klonuti, a oči se sklopiti, kao da je obuzima san.

"On traži žrtvu."

"I jeste li ju našli?"

"Nismo je morali tražiti, doktorice. Sami ste došli."

Odjednom, Barbara se bez glasa srušila. Očito, nije mogla više izdržati čudovišno djelovanje nepoznatih moći. Čeljusti su sad već bile na duljinu podlaktice od Honey. Iza stvora, prostorijom se razlijevao ritam drevne bajalice. Odakle im?

A onda se Honey trgne. Nije bilo vrijeme za pitanja.

Krik!

Barbarin.

Proparao je prostoriju i istjerao omamljenost iz Honeynog uma. Ona pograbi kovčeg s novcem, skoči iz stolice i njime zamahne prema čudovištu. Nije se obazirala na sedmorku koja je izletjela sa svojih stolica uz bijesne povike. Ali, zubati krak koji je šibao zrak iznad stola držao ih je podalje. Dobro su znali što ih čeka ako ih dohvati. A znala je i Honey, imala je prilike vidjeti. Tri čovjeka poginula su tog dana kad je doktor Henders otvorio kutiju. Očito, stvor se morao umilostiviti krvavom žrtvom. A sad ga je žrtva mlatila kovčegom.

Krak je zamahnuo prema Honey i istrgnuo joj kovčeg iz ruke. Odletio je u stranu i pao negdje u mrak.

"Da se ja zahvalim na gostoprimstvu", procijedila je Honey.

Htjela je potražiti kovčeg, pa van kroz vrata. Ali, zaustavilo ju je stenjanje. Barbarino. Ona pogleda u tamu, pa u mladu ženu sad raščupane kose. Pa onda opet u tamu, gdje je bio kovčeg. Shvatila je da neće stići izvući i Barbaru i kovčeg. Neman što je prskala slinu iz usta preko cijelog stola neće joj to dopustiti.

I zato Honey uhvati Barbaru za ruku i povuče prema vratima. Žena je jedva bila pri svijesti. Doktorica Hilger nije znala je li i ona trebala biti žrtva. Ne bi se začudila da je to bio Wittov plan. Povukla ju je na noge.

"Miči se!", povikala je Barbari u uho i to kao da ju je trgnulo. Nije više bila vreća krumpira. Njih dvije zaletjele su se prema vratima, tresnule o njih, dok se iza njihovih leđa stvor bacio na sedmorku. Krici užasa i boli ispunili su prostoriju. Honey zgrabi kvaku. I opsuje.

Naravno, vrata su bila zaključana.

"Kartica", procijedi Barbara i Honey se baci na njezine džepove. Ključ karticu pronašla je u unutarnjem džepu sakoa. Provukla ju je kroz utor na bravi. Činilo joj se da je prošla vječnost dok su se vrata, bez ikakve žurbe, otključala uz škljocaj.

Dok je gurala Barbaru kroz vrata, bacila je zadnji pogled na stol.

Stvor je upravo zubima komadao Witta. Dijelovi tijela prekrili su čitav stol. Krv se slijevala preko ruba. Što god sedmorka htjela od stvora, neće dobiti. Zagonetke ostaju neriješene, pitanja bez odgovora.

Honey zalupi vratima iza sebe. Prigušila su zadnje krikove. Uhvatila je Barbaru za ruku i povukla je prema izlazu. Odnekud je pritrčala srebrnasta batlerka.

"Ovdje je gotovo! Pođi s nama", zapovjedila joj je Honey.

Na izlazu, batlerka joj je pomogla obući kaput. Bez ikakve hitnje, taj trenutak činio joj se nestvarnim. Iza vrata više se ništa nije čulo. Honey je znala da se čudovište vratilo otkud je došlo. Kutija se sklopila, portal zatvorio.

I dok su njih tri išle ulicom, Honey se pokušavala prisjetiti broja ovdašnjeg čistača. Ovlaštenog da intervenira u ovakvim situacijama. Imat će puno posla dok napravi reda i osigura da kutija dođe u prave ruke.

Aleksandar Žiljak

Nastavak sa 16. stranice

Kerckhoffsov princip.

Što Eve mora napraviti kako bi ipak uspjela pročitati takvu poruku bez ključa? Ona mora provesti postupak kriptoanalize. Postupak kriptoanalize ili probijanje šifre općenito je jedan od najzahtjevnijih mentalnih postupaka koje ljudski mozak može podnijeti. Kriptoanaliza zahtijeva visoku razinu kognitivnih vještina: analiziranje šifri uključuje logičko razmišljanje, prepoznavanje uzoraka, matematičke i statističke vještine, što može biti mentalno vrlo zahtjevno. Gledano kroz povijest, probijanje šifri (npr. Enigma) zahtijevalo je iznimno talentirane matematičare i analitičare. Suvremena kriptoanaliza može uključivati složenu tehnologiju. Danas kriptoanalitičari koriste računalne algoritme i visokotehnološke alate, no za dizajniranje tih metoda još uvijek su potrebne znatne intelektualne sposobnosti.

Kako će Eve postupiti u prvom koraku? Vrlo vjerojatno brzo će zaključiti da tablice za šifriranje (tablica 1 ili 2) imaju konačan broj. Brojevi koji su "u igri" su konačni, a ima ih 26. Ako Eve ne zna kako sustav ove šifre funkcionira, ona bi to mogla zaključiti ako bi analizirala neku veliku količinu šifriranog teksta. Brzo bi uvidjela da se u nekoj šifri ne pojavljuju brojevi veći od 26, što bi aludiralo na to da su slova supstituirana brojevima.

Eve bi sada mogla pomisliti da broj 26 nije veliki broj, što bi značilo da se lako može doći do ključa. Ako prihvati takvu tvrdnju i krene sa svim kombinacijama koje broj 26 nudi, brzo će shvatiti da joj cijeli život neće biti dovoljan da isproba sve mogućnosti. Takav napad na šifru naziva se napad grubom silom (*Brute force attack*). Koliko kombinacija nudi broj 26, možemo izračunati računanjem faktorijela broja 26, što daje:

26! = 1 x 2 x 3 ... x 25 x 26 = 403291461126605635584000000 kombinacija.

Ako bi Eve u jednoj sekundi uspjela provjeriti jednu kombinaciju ključa, trebalo bi joj 12,78 trilijuna godina da provjeri sve kombinacije, odnosno sve ključeve i na taj način pronašla pravi ključ i dešifrirala poruku.

Iako sustav djeluje sigurno ako uzmemo u obzir broj godina koje Eve treba da bi provjerila sve moguće ključeve, stvarna sigurnost sustava nije toliko čvrsta ako se poznaju osnovni alati kriptoanalize, poput frekvencijske analize. Frekvencijska analiza je jednostavan alat pomoću kojeg bi se ova šifra mogla razbiti bez primjene napada grubom silom, koristeći samo "papir i olovku".

Međutim, treba napomenuti da napad grubom silom može biti ubrzan korištenjem uparenih računala, koja mogu paralelno testirati milijune kombinacija ključeva u vrlo kratkom vremenu. Stoga, iako bi u osnovi takva šifra bila izuzetno teška za dešifriranje, uparena računala omogućuju praktično rješenje šifre u mnogo kraćem vremenskom roku.

Sam postupak frekvencijske analize neće biti detaljno objašnjen u ovom članku, jer bi nas to odvelo izvan teme.

Upoznali smo se sa supstitucijskim šiframa, koje, kako samo ime kaže, mijenjaju jedno slovo otvorenog teksta u simbol, broj ili drugo slovo. U našem primjeru, slovo otvorenog teksta zamijenjeno je brojem.

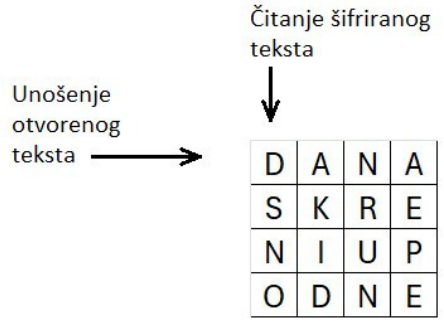
Transpozicijske šifre: Promjena poretka, a ne značenja

Kod transpozicijske šifre, slova otvorenog teksta ostaju kakva i jesu, ne mijenjaju se kao kod supstitucijskih, ali njihov položaj u poruci se mijenja prema nekom pravilu.

Pokazat ćemo primjer šifriranja rečenice "DANAS KRENI U PODNE".

Najjednostavniji oblik transpozicije je sustav zvan skitala, a njega su primjenjivali Spartanci u V. stoljeću pr. Kr. Tehnička izvedba takve naprave dostupna je na raznim internetskim stranicama, a ovdje će biti prikazana u općem obliku kao i svi ostali sustavi transpozicije, a to je tablični prikaz, ili, izraz što neki autori koriste, rešetka.

U prvom koraku napravimo tablicu dimenzije 4 x 4 jer naša poruka ima 16 slova. U tablicu zdesna nalijevo upisuju se slova otvorenog teksta kako je prikazano na slici 3.



Slika 3. Prikaz tablice (rešetke) za transpozicijski sustav Skitala za ključ 4

Sada se iz tablice iščitava tekst odozgo prema dolje kako je prikazano slikom 3. Tako dobivena poruka glasi:

DSNOA KIDNR UNAEP E

Možda se pitamo gdje je ključ za šifriranje, jer simetrični sustavi koriste ključ. Ključ je "ugrađen" u tablicu. U ovom slučaju ključ je 4 jer je tablica široka 4 slova, a budući da je duljina poruke 16 slova, tada jednostavnom matematikom možemo zaključiti da će i duljina biti 4 slova. Ako, primjerice, uzmemo da je ključ 8 tada dobijemo:

D	A	N	A	S	K	R	E
N	I	U	P	O	D	N	E

Slika 4. Prikaz tablice za transpozicijski sustav Skitala za ključ 8

Uz navedeni ključ 8 i isti otvoreni tekst prema istom sustavu, šifra će glasiti:

DNAIN UAPSO KDRNE E.

Jedna od prednosti ovakvog sustava je brzo šifriranje, a kako vidimo, Eve može kratke poruke lako razbiti.

Kako će Eve postupiti sa šifriranom porukom? Kao što smo se upoznali na početku, sustav šifriranja nije tajan i može se relativno lako saznati. Jedino ključ mora biti tajan. Budući da se sustav poznaje, Eve može znati da je broj ključeva onoliki koliko ima slova u poruci, a to je 16.

Pogledajmo koliko ključeva može biti učinkovito za ovakav način šifriranja. Primjećujemo da su sva slova iz poruke (njih 16) potpuno popunila tablicu. To znači da dimenzije tablice moraju biti višekratnici broja 16. Prema tome, tablica za poruku od 16 slova može imati dimenzije 1 × 16, 2 × 8, 4 × 4 ili 8 × 2.

Što ako poruka ima više ili manje slova? Tada poruka ima broj slova koji nije višekratnik odabranih dimenzija. To se može isto odnositi i na duljinu ključa, recimo 6. Pogledajmo kako se šifriranje odvija. Formirajmo tablicu duljine 6:

D	A	N	A	S	K
R	E	N	I	U	P
O	D	N	E		

Slika 5. Prikaz nepopunjene tabliceDobivena šifrirana poruka glasi: DROAE DNNNA IESUK P. Na ova prazna mjesta mogu se ubaciti nulta slova koja nemaju nikakvo značenje. Primjerice, možemo stavljati slovo x. Osobnog sam mišljenja da nam posebno lako uočljiva slova smanjuju sigurnost šifre, jer se u nekoj šifriranoj poruci lako vide, kao primjerice x u poruci pisanoj na hrvatskom jeziku. U takvom slučaju koristio bih rijetka slova hrvatskog jezika za popunjavanje, a to su slova G, H i V.

Jednom kada Alice takvu poruku pošalje nesigurnim kanalom, ona dolazi do Boba, ali i do Eve.

Prvi korak koji Bob radi je da koristi ključ koji ima za tu poruku, a to je ključ 6. U drugom koraku simulira unos šifriranog teksta duljine 16 slova:

1	2	3	4	5	6
7	8	8	10	11	12
13	14	15	16		

Slika 6. Prikazuje rekonstrukciju tablice koju provodi Bob

Bob sada popunjava tablicu tako da postupa obrnuto od Alice. Slova šifriranog teksta unosi istim redoslijedom kako je Alice iščitavala svoj uneseni otvoreni tekst. Na taj način Bob dobiva rekonstruiranu tablicu jednaku kakvu je imala i Alice.

Eve postupa tako da pokušava provesti sve kombinacije ključeva. Prvo se služi višekratnicima, a onda rekonstrukcijom koju je radio Bob. Na taj način, poznavanjem slabosti sustava, Eve pronalazi rješenje i razbija poruku bez upotrebe ključa. Ako bi poruka bila duža, Eve bi morala koristiti računalo jer su kombinacije u transpoziciji bitno manje nego one u sustavu supstitucijskih šifri.

Ovaj primjer transpozicijskog sustava, kao što je skitala, osnovni je transpozicijski sustav koji danas više služi za upoznavanje s klasičnom kriptografijom nego za sigurnu komunikaciju kao takvu.

Također je važno napomenuti da se iščitavanje unesenog teksta može provoditi tako da se poruka iščitava u raznim smjerovima. Slika 7 prikazuje razne načine iščitavanja kriptograma za isti ključ.

18	15	12	9	6	3
17	14	11	8	5	2
16	13	10	7	4	1

3	6	9	12	15	18
2	5	8	11	14	17
1	4	7	10	13	16

16	15	10	9	4	3
17	14	11	8	5	2
18	13	12	7	6	1

Slika 6. Prikaz ispisivanja šifriranog teksta prema unesenom otvorenom tekstu duljine 16 u rešetku s ključem 6

Nakon unošenja otvorenog teksta, kao što je prethodno opisano i prikazano na slici 6, šifrirani tekst se generira pomoću jednog od odabranih redoslijeda u tablici. Ipak, postoje razne varijante ispisivanja, ali mora se paziti da one ne odaju dijelove otvorenog teksta u šifriranoj poruci. Primjerice,spiralni princip koji je prikazan na slici 7.

8	7	6	5	4	3
9	18	17	16	15	2
10	11	12	13	14	1

Slika 7. Iščitavanje spiralnim postupkom

Ako bi otvoreni tekst bio prikazan nizom kako slijedi

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18

Slika 8. Unošenje otvorenog teksta u tablicu s ključem 4

tada bi nakon ispisivanja spiralnim nizom kako je prikazan slikom 7 šifrirani tekst bio ovaj prikazan na slici 8

18 12 06 05 04 03 02 01 07 13 14 15 16 17 11 10 09 08

Vidljivi dio poruke

Slika 9. Prikaz šifrirane poruke s ključem 6 ispisane spiralnim nizom

Iz primjera (slika 9) jasno je vidljivo da se dio poruke da odgonetnuti. Upravo to daje sumnju Eve da može očekivati još takvih ponavljanja ako je poruka veća. Na temelju takve informacije Eve može rekonstruirati tablicu otvorenog teksta.

Ovo je možda jednostavan i banalan primjer ponavljajućeg teksta u transpozicijskom šifriranju. Moram istaknuti da transpozicijski sustavi na neki način boluju od uobičajenih ponavljajućih dijelova u šifriranoj poruci, kako će doći do ponavljanja ovisi o duljini otvorenog teksta koji kriptoanalitičar (Eve) napada.

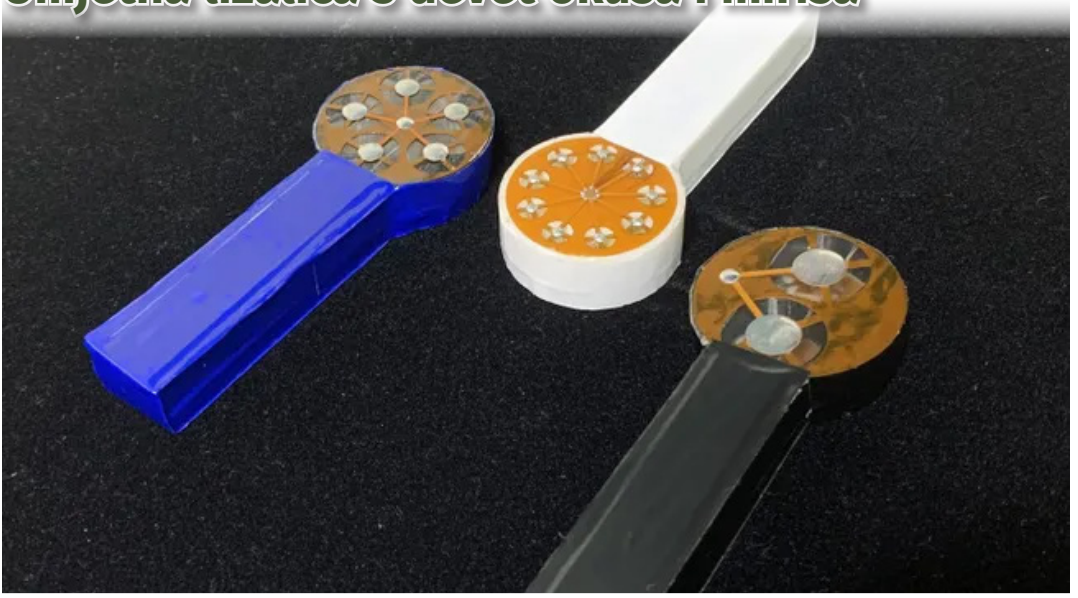
Povijesna važnost klasičnih šifri i njihova uloga danas

U ovom članku prikazana je osnovna podjela klasične kriptografije, a to čine supstitucijski i transpozicijski sustav. Iako su ti sustavi bili korišteni u samim počecima šifriranja, njihovi principi su temelj današnjih modernih kriptosustava.

Klasična kriptografija, premda danas povijesno važna, predstavlja temelj svih suvremenih kriptografskih sustava. Iako je tehnologija napredovala do neslućenih razina, osnovna načela poput supstitucije i transpozicije ostaju ključna u razumijevanju i dizajnu sigurnosnih algoritama. Osvrnemo li se na njihovu jednostavnost i genijalnost, vidimo kako i najjednostavnije ideje mogu oblikovati svijet. Ako vas je ovaj članak potaknuo na razmišljanje o šifriranju, možda ćete jednoga dana biti ti koji razvijaju nove sustave za očuvanje naše privatnosti u digitalnom dobu.

Dr. sc. Bojan Plavac

Umjetna lizalica s devet okusa i mirisa



Uređaji nalik "lizalici" omogućuju korisnicima da u virtualnoj stvarnosti "kušaju" do devet okusa.

Iskustva virtualne stvarnosti (VR) uskoro bi mogla postati puno realističnija zahvaljujući uređaju koji se može lizati i koji vam omogućuje "kušanje" u virtualnim okruženjima.

Malo sučelje nalik na lizalicu simulira do devet okusa i može se čak kombinirati s mirisima kako bi osjećaj okusa bio realan, kažu znanstvenici u novoj studiji nedavno objavljenoj u časopisu *PNAS*.

"U stvarnosti postoji pet tipičnih ljudskih osjeta – vid, zvuk, dodir, njuh i okus", prvi autor Yiming Liu, istraživač biomedicinskog inženjerstva na City Sveučilištu Hong Konga i Sveučilištu Tokija, kaže i dodaje: "Kako bismo razvili impresivno virtualno iskustvo za korisnike, nadamo se da ćemo korisnicima prikazati svih pet senzacija, gdje ćemo uspostaviti besprijekoran 3D-virtualni svijet (slično OASIS-u u filmu *Ready Player One*)."

Umjetna lizalica sadrži male vrećice napunjene gelovima. Ovi gelovi sadrže kemikalije koje, kada se pomiješaju sa slinom, simuliraju različite okuse koji uključuju sol, šećer, višnju, limunsku kiselinu, zeleni čaj, marakuju, grejp, durian i mlijeko.

Svaka aroma oslobađa se samo kada mala električna struja prođe kroz svaki pojedinačni gel, a isporučena količina ovisi o primijenjenom naponu. To znači da se nekoliko okusa može miješati kako bi se stvorili novi osjećaji okusa.

Osim što će igru virtualne stvarnosti učiniti impresivnijom, ovaj bi uređaj mogao imati praktične primjene, uključujući liječničke testove okusa, *online* kupnju namirnica i obrazovanje, sugerirao je tim.

Ovo nije prvi put da istraživači pokušavaju unijeti okus u virtualnu stvarnost. Drugi su istraživali izravnu primjenu kemikalija okusa na jezik i stimulaciju pomoću topline i struje.

Ovaj najnoviji razvoj nudi preciznu, niskoenergetsku opciju s kompaktnim, ručnim dizajnom. Međutim, Liu je primijetio da je tehnologija još uvijek u povojima i da ima ograničenja. Na primjer, gelovi trenutno traju samo oko sat vremena. Tim planira produljiti taj životni vijek i povećati broj dostupnih okusa.

Izvor: Yiming Liu
Tekst: www.livescience.com

Snježana Krčmar

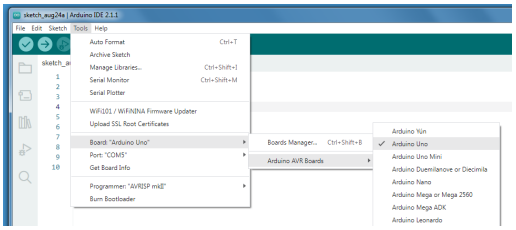
Starter kit Geekcreit UNO R3 (2)

U ovom ćemo nastavku naučiti kako instalirati programe Arduino IDE i Bascom-AVR, a napravit ćemo i jednostavan elektronički sklop i oživjeti ga prikladnim programom!

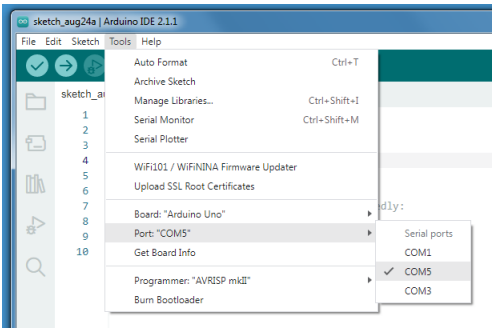
Instaliranje Arduino IDE

Arduino IDE je integrirano razvojno okruženje za programiranje mikroupravljača i mikroprocesora raznih porodica. Arduino IDE podržava programske jezike C i C++ sa zasebnim pravilima strukture programa. Pisan je u programskom jeziku Java što mu omogućuje lakšu prenosivost među operacijskim sustavima. Dostupan je za Windows XP i novije verzije te Linux, a može se besplatno preuzeti s internetske stranice *www.arduino.cc/en/software*. Trenutno je dostupna inačica 2.3.2. Za potrebe ove serije koristimo inačicu 2.1.1, a svi priloženi programi mogu se izvoditi i s novijim inačicama.

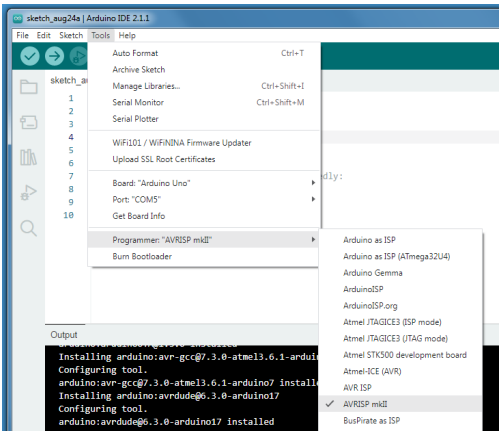
Tijekom instalacije, Arduino IDE instalira svu potrebnu programsku podršku kao što su *driveri* za komunikaciju s hardverskim programatorom preko USB porta i softverski programator *avrdude*. Po završenoj instalaciji Arduino IDE je potrebno konfigurirati tako da zna komunicirati s pločicom Arduino UNO. Konfiguracija se provodi pomoću padajućih izbornika *"Tools->Board"*, *"Tools->Port"* i *"Tools->Programmer"*. Način kako otkriti koji port su Windowsi dodijelili pločici Arduino je opisan u sljedećem poglavlju, "Instaliranje Bascom-AVR". Slike 5a, 5b i 5c prikazuju odabir pločice Arduino UNO, definiranje komunikacije pomoću USB *porta* i odabir softverskog programatora *"AVRISP mkII"*.



Slika 5a. Odabir pločice Arudino UNO



Slika 5b. Odabir komunikacije pomoću USB porta 4

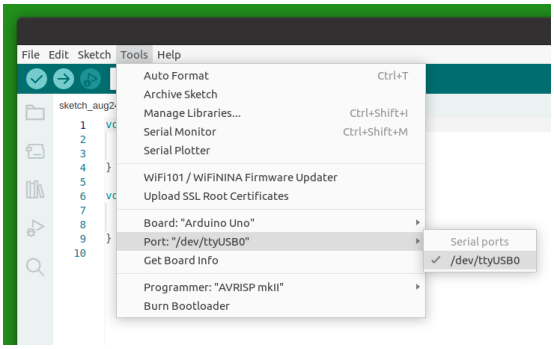


Slika 5c. Odabir softverskog programatora AVRISP mkII

Ukoliko ste instalirali Arduino IDE na operacijskom sustavu Linux, potrebno je uzeti u obzir da Linux dodjeljuje USB *portovima* drugačije oznake. U distribuciji za pronalaženje oznake porta Ubuntu Linux potrebno je pokrenuti emulator terminala pomoću kombinacije tipki CTRL-ALT-T te izvršiti naredbu *dmesg*:

```
$ dmesg
....
[  581.872302] usbserial: USB Serial support registered for ch341-uart
[  581.872317] ch341 1-6:1.0: ch341-uart converter detected
[  581.872679] usb 1-6: ch341-uart converter now attached to ttyUSB0
```

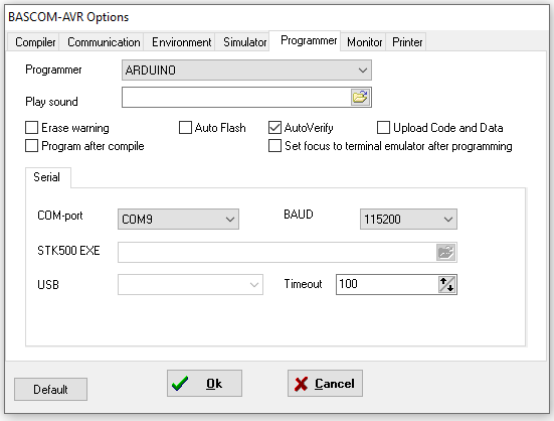
Iz primjera zaključujemo da je puna putanja do dodijeljenog porta */dev/ttyUSB0*. Na Slici 6 možete vidjeti odabir komunikacije pomoću USB porta 3.



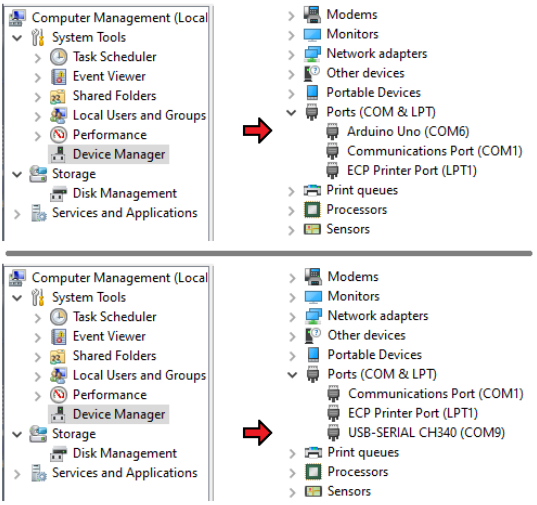
Slika 6. Odabir komunikacije pomoću USB *porta* 0

Instaliranje Bascom-AVR-a

Bascom-AVR je programski jezik i razvojni alat za programiranje mikroupravljača iz porodice AVR, što uključuje i ATmega328P s pločice Arduino Uno. Program se može instalirati na osobno računalo s operacijskim sustavom Windows verzije XP ili novije. Za nekomercijalnu primjenu dovoljna je demoverzija programa koja se može besplatno skinuti s internetske domene *mcselec.com*. Programi koje ćemo analizirati pisani su za Bascom-AVR demo 2.0.7.9, što je u ovom trenutku najviša dostupna demoverzija.



Slika 7. Postavke u izborniku Bascom-AVR-a Options-Programmer



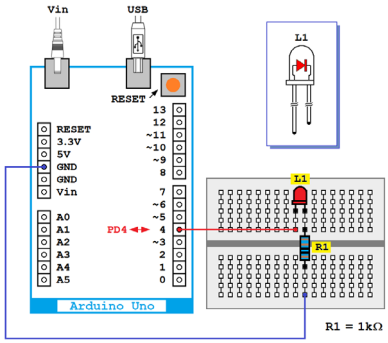
Slika 8. Ovako možete pronaći koji su COM port Windowsi dodijelili vašoj pločici Arduino UNO

Kada instalirate Bascom-AVR, potrebno ga je konfigurirati tako da zna komunicirati s pločicom Arduino UNO. Slika 7 prikazuje koje postavke treba upisati u izbornik *Options-Programmer*. Vrijednost u prozorčiću *COM port* ovisi o tome koji serijski port su Windowsi pridijelili programatoru s vaše pločice Arduino UNO. To možete saznati tako da povežete svoj Arduino UNO s USB portom osobnog računala i otvorite sučelje *Device Manager* (Slika 8). Kako ćete vidjeti svoju pločicu Arduino UNO ovisi o tome imate li originalnu izvedbu ili neki klon. Iako su funkcionalno (vjerojatno) identični, Windowsi vide male razlike pa će original prepoznati kako je prikazano na Slici 8 gore, a klon kao na Slici 8 dolje, možda i nekako drukčije. Nakon što ste u izbornik sa Slike 7 upisali odgovarajući broj *COM porta*, Bascom-AVR će ga zapamtiti i postupak nećete trebati ponavljati dokle god koristite istu pločicu Arduino UNO i isti USB port.

Sada, kada smo upoznali programe i opremu koju ćemo koristiti, vrijeme je da napišemo svoj prvi program.

1. programski zadatak

Svjetleću diodu L1, spojenu na Arduino UNO prema shemi na Slici 9, treba naizmjenično paliti i gasiti, tako da svako od tih stanja traje po jednu sekundu.



Slika 9. Shema spoja za prvi programski zadatak

Na Slici 9 vidimo kako je pin 4 pločice Arduino UNO spojen na anodu svjetleće diode L1, njena katoda spojena je s otpornikom, a drugi kraj tog otpornika spojen je na GND pločice Arduino UNO. Kod svjetlećih dioda izvod katode je kraći od izvoda anode, a donji rub kućišta zarezan je kod izvoda katode (ovo posljednje moći ćete uočiti i na crtežu na Slici 9).

Program Geekcreit_1.ino (Arduino IDE)

Program pisan u Arduino IDE sastoji se od najmanje dvije obavezne funkcije: *setup()* i *loop()*. Funkcija *setup()* izvršava se samo jednom, kod uključenja napona napajanja ili nakon *reseta* pločice Arduino UNO, i u njoj konfiguriramo pinove i definiramo komunikaciju s elektronskim sklopovima spojenima na pločicu Arduino UNO. Funkcija *loop()* je beskonačna petlja, koja se izvršava dokle god je Arduino UNO uključen. U sebi sadrži programski kod koji želimo izvršavati, a može po potrebi pozivati i dodatne funkcije. Obje funkcije ne vraćaju nikakvu vrijednost pa se stoga definiraju kao funkcije vrste *void*.

Sada pristupamo rješenju programskog zadatka. Kako su svi pinovi "prirodno" postavljeni kao digitalni ulazi, u funkciji *setup()* moramo pin 4 konfigurirati kao izlazni:

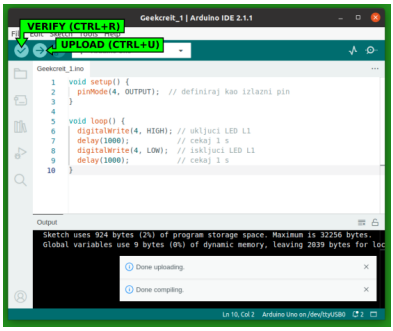
```
void setup() {
  pinMode(4, OUTPUT);      // definiraj kao izlazni pin
}
```

Sada će logičko stanje pina 4 imati direktan utjecaj na svjetleću diodu L1. To stanje ćemo mijenjati u funkciji *loop()*, pa će se dioda naizmjenično uključivati i isključivati dokle god je mikroupravljač spojen na napon napajanja (ili dok ne obrišemo program):

```
void loop() {
  digitalWrite(4, HIGH); // uključi LED L1
  delay(1000);           // čekaj 1 s
  digitalWrite(4, LOW);  // isključi LED L1
  delay(1000);           // čekaj 1 s
}
```

Naredba *delay(1000)* zadržava izvršenje programa 1000 milisekundi, odnosno jednu sekundu, kako bi periodi "svijetli" i "ne svijetli" odgovarali zahtjevu postavljenom u programskom zadatku.

Kada smo napisali program, moramo provjeriti ispravnost sintakse i prevesti ga u strojni kod koji mikroupravljač "razumije" (kombinacija tipki Ctrl-R ili klik na gumb *Verify*) te ga zatim prenijeti u mikroupravljač (kombinacija tipki Ctrl-U ili klik na gumb *Upload*). Ako ne pritisnemo gumb *Verify*, pritiskom na tipku *Upload* ujedno će se pokrenuti i provjera ispravnosti, prijevod programa i prijenos programa u mikroupravljač, pod uvjetom da je sintaksa programa ispravna. Slika 10 prikazuje gumbe *Verify* i *Upload* u programskom sučelju.



Slika 10. Arudino IDE s oznakama gumba *Verify* i *Upload*

Nakon uspješnog prijenosa programa u mikroupravljač, u donjem se dijelu prozora Arduino IDE pojavljuje poruka "*Done uploading.*" i uskoro će se dioda L1 početi naizmjenično uključivati i isključivati, što nam je potvrda da smo naš program dobro napisali.

Program Geekcreit_1.bas (Bascom-AVR)

Struktura programa pisanog u programskom jeziku Bascom-AVR ponešto se razlikuje od programa pisanog u Arduino IDE. Ponajprije, svaki program pisan u programskom jeziku Bascom-

AVR ima uvodni dio, u kojem prevodiocu "objašnjavamo" za koji mikroupravljač program pišemo, na kojoj brzini on radi te dajemo upute, kako koristiti memoriju mikroupravljača:

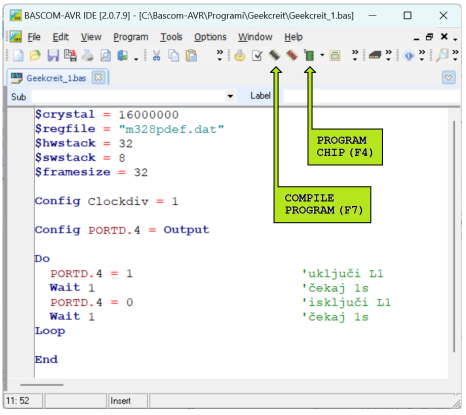
```
$crystal = 16000000
$regfile = "m328pdef.dat"
$hwstack = 32
$swstack = 8
$framesize = 32

Config Clockdiv = 1
```

Ovaj uvodni dio bit će identičan u svim programima koje ćemo pisati. Zatim ćemo pin 4, na koji je spojena svjetleća dioda, proglasiti izlaznim. Bascom-AVR ne poznaje oznake priključaka na pločici Arduino UNO, nego ćemo morati izlaznim konfigurirati pin mikroupravljača koji je s njim povezan, Portd.4 (skraćeno, PD4):

```
Config Portd.4 = Output
```

Konačno, u beskonačnoj petlji *Do...Loop* naizmjenično ćemo postavljati taj pin u stanje logičke jedinice i logičke nule, kako bismo svjetleću diodu naizmjenično uključivali i isključivali:

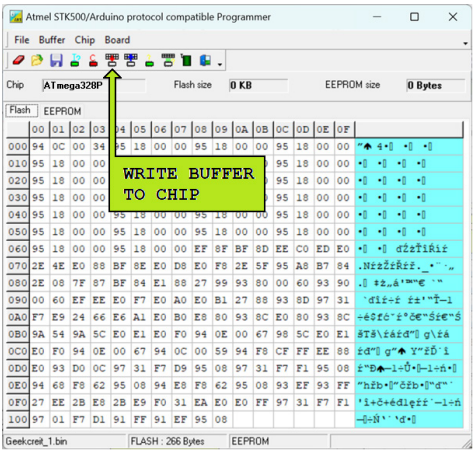
```
Do
  Portd.4 = 1  'uključi L1
  Wait 1       'čekaj 1s
  Portd.4 = 0  'isključi L1
  Wait 1       'čekaj 1s
Loop
```



Slika 11. Osnovni prozor Bascom-AVR-a s editorom za unos programa i gumbima za izvršenje različitih naredbi

Naredba *Wait 1* zadržava izvršenje programa u trajanju od približno jedne sekunde, kako bi svjetleća dioda žmirkala u zadanom ritmu.

Kada smo napisali program, moramo ga prevesti (F7 ili klik na gumb *Compile program*) i zatim prenijeti u mikroupravljač (F4 ili klik na gumb *Program chip*). Slika 11 prikazuje gdje se navedeni gumbi nalaze u programskom sučelju.



Slika 12. Bascom-AVR prozor za komunikaciju s programatorom

Gumb *Program chip* otvara novi prozor pomoću kojega komuniciramo s programatorom na pločici Arduino UNO (Slika 12). Ovdje vidimo tablicu s nizom heksadekadskih brojeva, koji predstavljaju naš program u obliku koji razumije mikroupravljač. Programiranje mikroupravljača počet će kada kliknemo na gumb *Write buffer to chip*. Proces traje nekoliko sekundi i, čim se u prozorčiću *Chip* pojavi naziv mikroupravljača (ATmega328P), to će biti znak da je Bascom-AVR uspio uspostaviti komunikaciju s čipom za programiranje na pločici Arduino Uno. Uskoro će dioda L1 početi žmirkati, što nam je potvrda i da smo naš program dobro napisali.

U sljedećem ćemo nastavku puno više programirati! Do čitanja!

Napomene: Članak je izvorno objavljen u slovenskom časopisu *Svet elektronike*. Za objavljivanje u časopisu *ABC tehnike* prilagodili autori. Programe Geekcreit_1.ino i Geekcreit_1.bas možete besplatno dobiti od uredništva časopisa *ABC tehnike*.

Vladimir Mitrović i Robert Sedak

Praksa ratnih robota

Već smo nekoliko puta u ovom 25 godina dugom serijalu pisali o vojnim primjenama robota, ali to su uglavnom bili opisi pojedinačnih strojeva na ispitnim poligonima ili oni rijetki koji su imali uporabnu perspektivu. Nikada nismo svjedočili masovnom korištenju ratnih robota. Neke vrste robota s primjenama vezanim uz rat koriste se vrlo uspješno pojedinačno već nekoliko desetljeća. Takvi su veliki dronovi poput MQ Predatora za izviđanje ili uništavanje izoliranih ciljeva u ratnim operacijama. Slično je i s robotima za uočavanje i uklanjanje formacijskih mina.

No nikada prije ukrajinskog rata nije se dogodilo da se ratni roboti koriste masovno do mjere da učestalost njihove uporabe mijenja taktiku, pa i strategiju ratovanja kakvu smo prije poznavali. Britanski Royal United Services Institute procijenio je da je Ukrajina znala gubiti i do 10000 bespilotnih letjelica mjesečno. To upućuje da se koriste milijunske količine letećih dronova. Najviše je vrlo malih kvadkoptera veličine desetak centimetara, preuređenih dodavanjem eksploziva u tzv. lutajuće streljivo, do onih velikog dosega s rasponom krila većim od 15 metara. Mali dronovi imali su posebno važnu ulogu u Ukrajini, a njihova izuzetnost bila je potvrđena u veljači 2024., kada je predsjednik Volodimir Zelenski odredbom osnovao "Snage bespilotnih sustava" koje se isključivo bave razvojem i ratnim primjenama zemaljskih, zračnih i morskih robota. Ukrajina je do kraja 2024. godine proizvela više od milijun bespilotnih letjelica.

Novčani volumen tržišta vojnih robota procijenjen je u 2022. na 13,4 milijarde američkih dolara. Rast će po stopi od preko 8,5% između 2023. i 2032. jer tržište vojnih robota pokreće potreba za autonomnim oružjima u modernom ratovanju. Oni smanjuju ratne rizike za vojnike i povećavaju vjerojatnost uspješnosti akcija. Ratni roboti postali su element stjecanja strateške prednosti na bojnom polju.

Vojni roboti bit će još masovnije i učinkovitije primjenjivani u bliskoj budućnosti za provođenje potraga, nadzora, izviđanja, prikupljanja informacija, špijuniranja lokacije, probijanja neprijateljskih sigurnosnih linija, kao i za izravno pružanje podrške na bojnom polju. Moderno ratovanje temeljit će se sve više na autonomnom oružju i robotiziranim vojnim sustavima.

Buduće ratovanje od vojnika će sve više zahtijevati rad s autonomnim i poluautonomnim strojevima. Izravno pucanje će se smanjivati. Koncept robotike u oblaku i računalstva u oblaku temeljenim na internetu stvari učinit će ratne strojeve moćnijima u smislu obrade podataka, pohrane informacija, dijeljenja i analize informacija, donošenja odluka, automatiziranog planiranja borbe, pa i izvođenja zaključaka. Riječju, oblak će držati vojni mozak budućnosti ratovanja.

Vojni roboti svrstavaju se u tri grupe: bezposadna kopnena vozila (engl. skraćenica *UGV*),

RATNI "GAME CHANGERI". Brojne zemlje nastoje razviti i proizvoditi borbene daljinski vođene i autonomne bespilotne sustave. Nalazimo ih u sve većem broju kod svih rodova vojske: od zračnih dronova različitih veličina, preko zemaljskih izviđačkih ili naoružanih vozila do plovila ili podmornica. Na slici lijevo prikazan je ukrajinski ubojni pomorski dron "Avdika" namijenjen uništavanju brodova. Slika u sredini prikazuje roj vojnih kvadkoptera koji bi u perspektivi smanjenjem veličine i povećanjem brojnosti mogao dovesti do nestanka skupih tenkova. Američka agencija DARPA podupire razvoj programa "Taktika ofenzivnog roja" za opremanje vojnika rojevima do 250 bespilotnih letjelica i zemaljskih vozila. Slično bi se moglo događati i s morskim dronovima. Veliki oklopni kopneni dronovi poput ruskog tenka "Uran-9", na slici desno, uvedeni su u uporabu za sirijskog građanskog rata.



KOPNENI DRONOVI. Među kopnenim robotima vrlo su tražene tzv. "robotičke mule", autonomne inačice slavnih kamiona James ili malih Jeepova. Na slici lijevo je SMSS (*Squad Mission Support System),* autonomno kopneno vozilo koje proizvodi Lockheed Martin. To je najveći autonomni kopneni robot raspoređen u američkoj vojsci. U sredini je robotički kamion R-Gator tvrtke za proizvodnju autonomnih poljoprivrednih strojeva John Deer. Može djelovati autonomno prateći kartu, odrediti vlastite pozicije kako bi stigao do odredišta ili "pratiti vođu" u konvoju da bi išao ukorak s trupama. Može biti daljinski upravljan, ali ga se može voziti i ručno. R-Gator služi za nošenje opreme za vojnike, ali i za postavljanje na radnu poziciju malih robota za uklanjanje eksplozivnih sredstava teških više od 45 kg.

bespilotne letjelice (engl. skraćenica *UAV*) i besposadna površinska plovila i dronovi podmornice (engl. skraćenica *UUV*). Za sve njih koristio se u početku pojam "dron" koji je naknadno prevladao kod letjelica. Posljednjih godina pod utjecajem ukrajinskog rata počinje se vraćati jedinstveni pojam dron.

Bespilotne letjelice (UAV) su dronovi koji se koriste za nadzor, izviđanje i ciljane napade. Njihova agilnost omogućuje brzo prikupljanje podataka i donošenje odluka na bojištu u stvarnom vremenu, što ih čini nezamjenjivima u borbi.Bespilotna kopnena vozila (UGV) koriste se za zadatke u rasponu od logistike i prijevoza opskrbe do odlaganja eksplozivnih sredstava, čime se smanjuje rizik za ljudsko osoblje.

Mornarički dronovi djeluju u pomorskim okruženjima za misije kao što su izviđanje, otkrivanje mina i protupodmorničko ratovanje. Ova plovila poboljšavaju pomorske sposobnosti proširujući domet i trajnost operacija bez ugrožavanja sigurnosti brodova s posadom. Svaki od ovih robotskih sustava igra vitalnu ulogu u unapređenju vojne učinkovitosti u borbenim scenarijima.

Globalno tržište ratne robotike geografski je segmentirano u pet glavnih regija: Sjeverna Amerika, Europa, Azija i Pacifik, Bliski istok i Afrika te Latinska Amerika.

U 2019. godini veličina europskog tržišta vojnih robota iznosila je blizu pet milijardi USD, što je najveći udio na tržištu zahvaljujući prisutnosti velikih proizvođača koji posluju na tom tržištu. Prema izvještaju portala *The World Robotics*, od ukupno više od 700 tvrtki za proizvodnju servisnih robota identificiranih diljem svijeta, gotovo polovina poslovala je u Europi. Europa ima snažnu kontrolu nad integracijom širokog spektra tehnologija. To uključuje govorno i haptičko sučelje čovjek–stroj, navigaciju i izbjegavanje sudara, planiranje kretanja i zadataka i drugo obrambeno planiranje u 2020. godini.

Nakon Europe, očekuje se da će azijsko-pacifička regija u nadolazećim godinama rasti eksponencijalno u opremanju ratnim robotima. To je uglavnom posljedica kineskih ulaganja u vojne programe za zračnu, kopnenu i pomorsku obranu. Kina i Indija povećavaju ulaganje u



KOPNENI NAORUŽANI DRONOVI. Bespilotna kopnena vozila THeMIS (slika lijevo) naoružana hibridnim pješačkim sustavima koje je izgradila estonska tvrtka Milrem Robotics. Koristi ga više članica NATO-a. Nizozemska i Estonija prednjače u testiranju naoružanih robotskih vozila unutar NATO saveza no posljednjih godina i američka vojska testira lagana, srednja i velika robotska borbena vozila opremljena topom XM813 Bushmaster, mitraljezima kalibra 12,5 i bacačima projektila FGM-148 Javelin (slika desno). U sredini je kineski mali borbeni robot "Sharp Claw" naoružan teškom strojnicom.



PODVODNI DRONOVI. Mornarički podvodni dron “GhostSwimmer” (slika lijevo) težak je oko 100 kilograma, otprilike je veličine tune, ali više sliči morskom psu. To je dio istraživanja mogućnosti biomimetičkih, bespilotnih, podvodnih vozila. Robot za pogon koristi rep. Može raditi u plitkoj vodi od 25 cm ili roniti do 90 m, upravljanje je daljinsko preko žice dugačke do 150 m, ili samostalno plivati, povremeno se vraćajući na površinu radi komunikacije. Robotska riba je neprimjetna: izgleda kao riba i kreće se poput ribe pa se teško uočava. “Manta Ray” Northrop Grummana, nalik divovskoj raži (slika desno), podvodni je dron dugog dometa za "klizanje vođeno plovnošću za kretanje kroz vodu" i ima više prostora za teret za podršku raznim misijama. Opremljen je sustavom koji izvlači energiju iz toplinskog gradijenta oceana i pretvara ga u električnu energiju; plovilo može dugo prikriveno ležati usidreno na morskom dnu i hibernirati. Pomorski dronovi projektirani su kao podmorska ili površinska plovila. No dron “Triton” (slika u sredini) tvrtke Ocean Aero, hibridno je plovilo koje jedri i roni pokretano vjetrom i solarnom energijom. Može roniti i do dubine od 200 m.

razvoj koje će iz temelja promijeniti sposobnosti vojnih robota.

Značajan trend u industriji vojnih robota je integracija sposobnosti umjetne inteligencije i strojnog učenja što omogućuje robotima prilagodbu promjenjivim okruženjima, samostalno donošenje odluke i poboljšanje ukupnih svojstava. Vojni roboti opremljeni umjetnom inteligencijom mogu analizirati ogromne količine podataka u stvarnom vremenu, poboljšavajući uvid vojnog osoblja u stanje bojišta i donošenje odluka. Ovi se roboti mogu prilagoditi dinamičnim i nepredvidivim okruženjima usklađujući svoje aktivnosti s podacima u stvarnom vremenu što ih čini učinkovitijima u izviđačkim ili borbenim misijama. Roboti su autonomni čime se smanjuju potrebe za stalnim ljudskim nadzorom i intervencijama. To omogućuje vojnicima da se usredotoče na strateške zadatke više razine dok se roboti bave rutinskim ili opasnim operacijama.

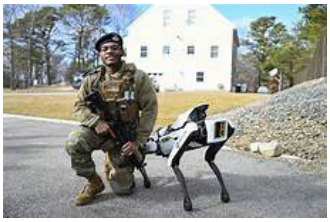
> Roboti se sve više koriste u ukrajinskim sukobima. Krajem 2024. Ukrajina je izvela uspješan napad na ruske položaje u blizini Lipšija, sjeverno od Harkova koristeći samo zemaljske robote s automatskim oružjima i leteće dronove. (Guardian, veljača 2025.)

Prema predviđanjima površinska autonomna vozila i robotski oružani sustavi vojske SAD-a mogli bi uskoro činiti oko 60% ukupnih sredstava. Kina sve snažnije sudjeluje u razvoju vojne robotike i predviđa se njena vodeća uloga jer postoji podrška s najviših razina kineske politike.

Rusija je iskoristila svoju vojnu intervenciju u Siriji kako bi testirala razne bespilotne kopnene letjelice za buduće vojne primjene, uključujući i nenaoružani dron za čišćenje mina “Uran-6” i



OBRANA OD LETEĆIH DRONOVA. Laseri i akustični udarni valovi koriste se za obranu od letećih dronova. Sustav HELWS (slika lijevo) koji je proizveo Raython ima visokoenergetski laser postavljen na pustinjski vojni bagi koji još uvijek ima dva prednja sjedala, a straga je sustav napajanja i ciljanja. Na slici u sredini prikazan je dron sa spaljenim propelerima. Na terenu se HELWS baterijski napaja. Akustični integrirani sustav tvrtke Epyrus na slici desno, nazvan Stryker Leonidas, pokazao je na poligonskim ispitivanjima potencijalnu učinkovitost onesposobljavanja dronova koji djeluju pojedinačno ili u rojevima.



ROBOTIČKI PSI I LUTAJUĆE GRANATE. Sitni "Drone 40" (slika u sredini) pripada grupi dronova koje nazivaju i lutajuće streljivo. Koristi se za skupljanje podataka, nadzor i izviđanje jer ima kameru čije se video snimke prenose na tablet vojnika. Dron najprije izviđa neprijateljske položaje, a zatim ga se u narednom letu pošalje kao granatu. Napaja se baterijama, a u zraku može provesti između 30 i 60 minuta. Leti brzinom od oko 50 km/h. Ispitivanje uporabe robotičkih pasa u američkim vojnim vježbama pokazaloje da poluautonomni robotski psi još nisu za korištenje u borbama pa se istražuje njihova korisnost u nadzoru i logistici (slika lijevo). Velike tvrtke koje stoje iza razvoja kvadripeda predvođene Boston Dynamicsom napisale su u listopadu 2024. godine otvoreno pismo u kojem se protive potencijalnom naoružavanju tih strojeva. Takve moralne akcije nisu imale utjecaj na kinesku vojnu propagandu čiji su roboti sa strojnicama na leđima preplavili internet (slika desno).

teško naoružani robotski tenk "Uran-9" namijenjen za izviđanje i vatrenu potporu. Rusko Ministarstvo obrane objavilo je 2021. godine da su prvi put koristili robote "Uran-9" u manevrima, a godinu dana poslije, ruska vojska rasporedila je "Uran-6" za potporu snajperskim jedinicama u regiji Luhansk.

U ukrajinskom ratu najveću operativnu potvrdu dobili su leteći i pomorski dronovi. Ukrajinski dronovi zaustavili su prve napade oklopnih snaga nadomak Kijeva, dok su na moru potisnuli Rusku mornaricu iz Crnog mora potopivši neke vrlo skupe brodove poput krstarice "Moskva". S druge strane, jeftini dronovi iranske proizvodnje "Shahid" korišteni su za teroriziranje civilnog stanovništva širom Ukrajine.

Samo nekoliko tjedana nakon što je objavljeno otvoreno pismo proizvođača robotskih pasa o etici njihove uporabe pojavio se video kineske obrambene tvrtke "Kestrel Defense" u kojem bespilotna letjelica spušta na krov robotskog psa s kineskim lakim mitraljezom na leđima. Robotski psi poslužili su Kinezima kao propagandno sredstvo. I Rusija je uvidjela robotičku budućnost ratovanja što se vidi iz njihove izjave da će lider na polju umjetne inteligencije biti vladar budućeg svijeta. Razmatranje korištenja ratnih robota ne podrazumijeva danas samo njihovu ofenzivnu napadačku ulogu. Sve je važnija i zaštita od dronova. Posebice se to vidjelo na dosadašnjim vladarima ratovanja od II. svjetskog rata naovamo: tenkovima. Dronovi su postali tzv. lutajuća vrsta streljiva s promjenjivom putanjom.

O širenju praktičnog korištenja ratnih robota najbolje svjedoči razvoj sredstava obrane od letećih dronova. Postoje četiri načina obrane. Prvo je fizičko pojedinačno uništavanje dronova različitim vrstama oružja i streljiva. Na tenkovima se koriste zaštitne mreže koje sprječavaju izravan udar. No taj način postaje neučinkovit kod masovnog korištenja letjelica. Moderniji način je uništavanje pokretnim laserom kojim se spaljuju vitalni dijelovi poput propelera. Sličan način je korištenje snažnih zvučnih valova. To su nedovoljno u praksi ispitane metode.

U praksi se koriste radiofrekvencijski analizatori koji ometaju bežičnu vezu robota i operatera ili se preuzima kontrola nad dronom koji kontrolirano slijeće u svom trenutnom položaju, vraća na svoju polaznu programiranu kućnu lokaciju, nekontrolirano pada na tlo ili odleti u nasumičnom smjeru. Na taj način mogu se dosta uspješno onemogućiti teleoperacijska sredstva, a kao obrana od radiooometanja počelo se koristiti žične veze s vrlo tankim vodičima informacija.

Igor Ratković

Može li umjetna inteligencija kopirati vašu osobnost?

Agentima umjetne inteligencije treba samo 2 sata da repliciraju vašu osobnost s 85 posto točnosti

Sve što je potrebno da se napravi točna replika nečije osobnosti je dvosatni razgovor s modelom umjetne inteligencije (UI), otkrili su istraživači.

U novoj studiji, u bazi podataka za preprint baze podataka arXiv, istraživači s Googlea i Sveučilišta Stanford stvorili su "agente simulacije" – replike umjetne inteligencije – od 1052 osobe na temelju dvosatnih intervjua sa svakim sudionikom. Ovi intervjui korišteni su za treniranje generativnog modela UI osmišljenog da oponaša ljudsko ponašanje.

Kako bi se procijenila točnost AI replika, svaki je sudionik završio dva kruga testova osobnosti, društvenih anketa i logičkih igara, te su zamoljeni da ponove postupak dva tjedna kasnije. Kada su replike umjetne inteligencije bile podvrgnute istim testovima, odgovarale su odgovorima svojih ljudskih kolega s 85 posto točnosti.

Simulacija ljudskih stavova i ponašanja

Navodi se da bi modeli umjetne inteligencije koji oponašaju ljudsko ponašanje mogli biti korisni u različitim scenarijima istraživanja, kao što je procjena učinkovitosti javnih zdravstvenih politika, razumijevanje odgovora na lansiranje novog proizvoda na tržište ili čak modeliranje reakcija na važne društvene događaje koji bi inače mogli biti preskupi, izazovni ili etički presloženi za proučavanje s ljudskim sudionicima.

"Općenamjenska simulacija ljudskih stavova i ponašanja, gdje se svaka simulirana osoba može uključiti u niz društvenih, političkih ili informacijskih konteksta, mogla bi omogućiti laboratoriju za istraživače da testiraju širok skup intervencija i teorija", kažu istraživači. Simulacije bi također mogle pomoći u osmišljavanju novih javnih intervencija, razviti teorije o uzročnim i kontekstualnim interakcijama i povećati naše razumijevanje načina na koji institucije i mreže utječu na ljude.

Kako bi stvorili agente simulacije, istraživači su proveli temeljite intervjue koji su obuhvatili životne priče sudionika, vrijednosti i mišljenja o društvenim pitanjima. To je omogućilo umjetnoj inteligenciji da uhvati nijanse koje tipične ankete ili demografski podaci mogu propustiti. Što je najvažnije, struktura ovih intervjua dala je istraživačima slobodu da istaknu ono što smatraju najvažnijim za njih osobno.

Znanstvenici su koristili ove intervjue za generiranje personaliziranih modela umjetne inteligencije koji mogu predvidjeti kako bi pojedinci mogli odgovoriti na anketna pitanja, društvene eksperimente i igre ponašanja. To uključuje odgovore na Opću društvenu anketu, dobro uspostavljen alat za mjerenje društvenih stavova i ponašanja Inventar ličnosti i ekonomske igre poput Igre diktatora i Igre povjerenja.

Pogreške i mogućnost zlouporabe

Iako su agenti umjetne inteligencije u velikoj mjeri odražavali svoje ljudske kolege u mnogim područjima, njihova točnost varirala je ovisno o zadacima. Posebno su se dobro pokazali u repliciranju odgovora na ankete o ličnosti i određivanju društvenih stavova, ali su bili manje precizni u predviđanju ponašanja u interaktivnim igrama koje uključuju donošenje ekonomskih odluka. Istraživači su objasnili da se umjetna inteligencija teže snalazi u zadacima koji uključuju društvenu dinamiku i kontekstualne nijanse.

Također su priznali mogućnost zlouporabe tehnologije. UI i *deepfake* tehnologije već koriste zlonamjerni ljudi za prevaru, lažno predstavljanje, zlostavljanje i manipuliranje drugim ljudima na internetu. Agenti simulacije također se mogu zloupotrijebiti, rekli su istraživači.

No, kažu i da bi nam tehnologija mogla omogućiti proučavanje aspekata ljudskog ponašanja na načine koji su prije bili nepraktični, pružajući visoko kontrolirano testno okruženje bez etičkih, logističkih ili međuljudskih izazova rada s ljudima.

Glavni autor studije Joon Sung Park, doktorand računalnih znanosti na Stanfordu, kaže: "Ako možete imati hrpu malih verzija vas koje trče uokolo i zapravo donose odluke koje biste i vi donijeli, mislim da je to u konačnici budućnost."

Izvor: Paper Boat Creative/Getty Images

Tekst: www.livescience.com

Snježana Krčmar