EDUTORIJ

Nastavnička priprema

Uvod u RSA kriptografiju

Osnovni podaci

ID: 4458440

Jezik: hrvatski - standardni

Materijal je recenziran: Ne

Status: Gotov materijal

Opis: Ovaj je materijal namijenjen za rad s darovitim učenicima. Cilj materijala je uočiti povezanost matematike i računalne sigurnosti, primijeniti dijeljenje s ostatkom pri stvaranju jednostavnih ključeva, koristiti digitalne alate za izvođenje matematičkih izračuna.

Kategorija:

Obrazovni sadržaji-> Osnovne škole-> 5. razred-> Matematika-> A. Brojevi-> MAT OŠ A.5.2. Rastavlja broj na proste faktore i primjenjuje djeljivost prirodnih brojeva

Doprinositelji

Ime: Dubravka Despoja
Uloga: Osobe ili ustanove koje objavljuju materijal
Autor: Ne
Registrirani korisnik: Da

Ime: Dubravka Despoja
Uloga: autor
Autor: Da
Registrirani korisnik: Da

Ime: Vjekoslav Jakopec
Uloga: autor
Autor: Da
Registrirani korisnik: Da

Edukacijski podaci

Vrsta: Priprema za nastavni sat

Kome je materijal namijenjen: učiteljima i nastavnicima

Razina interaktivnosti: visoka razina interaktivnosti

Namjenjena dob:

> **Dobni raspon:** starija osnovnoškolska dob
> **Vrijeme učenja:** jedan do tri sata

Znanja koja će učenici steći: Primijeniti dijeljenje s ostatkom pri stvaranju jednostavnih kriptografskih ključeva. Objasniti razliku između javnog i privatnog ključa. Povezati matematiku i sigurnost na internetu. Koristiti digitalne alate za istraživanje matematičkih problema.

Tehnički podaci

Pristup i licenciranje

Plaćanje: ne

Uvjeti iskorištavanja materijala: Imenovanje (CC BY)

Način pristupa: Otvoreni pristup

Namjena pripreme

> **Opis aktivnosti:** Razgovaramo s učenicima: ″Koristite li lozinke? Što bi se dogodilo da svi znaju vašu lozinku? Kako Internet štiti podatke?″ Navodimo primjer internetske kupnje i internetskog bankarstva. Upoznajemo učenike s razvojem kriptografije od Cezarove šifre do suvremenih metoda zaštite podataka.
> **Aktivnost:** Uvodni dio (15 min)

> **Opis aktivnosti:** Kriptografski algoritmi su matematičke metode i postupci koji se koriste za osiguranje povjerljivosti podataka. Kriptografski algoritmi mogu se grubo podijeliti na dvije vrste: simetrični koji koristi jedan ključ i asimetrični koji koristi dva ključa (javni i privatni). RSA je asimetričan algoritam (autori Rivesta, Shamira i Alderman) koji se oslanja na modularnu aritmetiku. U asimetričnim algoritmima jedan ključ služi za šifriranje, a drugi za dešifriranje.
> **Aktivnost:** Što je RSA? (10 min)

> **Opis aktivnosti:** Na primjer, učenik Marko želi primati šifrirane poruke od 10 svojih prijatelja. Ukoliko koristi simetričan algoritam tada sa svakim prijateljem mora dijeliti ključ. To znači da mora imati 10 različitih ključeva, za svakog prijatelja drugi. Međutim, ako koristi

asimetričan algoritam Marko će svojim prijateljima podijeli isti ključ (zato ga zovemo javni). Sa svojim ključem, kojeg zna samo on (zato se zove privatni) može dešifrirati poruke svakog svog prijatelja dok prijatelji međusobno ne mogu izmjenjivati poruke. U RSA algoritmu javni i privatni ključ sastoji se od uređenog para brojeva. Npr. ako je javni ključ (5,14) privatni ključ također može biti (5,14), ali i (11,14), (17,14),... Postupak za dobivanje ključeva je sljedeći: Korak 1:Izaberemo dva prosta broja, npr. p = 2 i q = 7. Izračunamo njihov umnožak n = p · q = 2 · 7 = 14. Korak 2: Izračunamo Eulerovu funkciju E(n) = (p − 1) • (q − 1) = 1 • 6 = 6 i odaberemo broj e koji je manji od 6 i nema zajedničkih faktora sa 6, npr. e = 5. Javni ključ je uređeni par (e, n), tj. (5, 14). Korak 3: Određujemo privatni ključ računajući broj d tako da vrijedi (d • n)(mod E(n)) = 1 tj. u našem primjeru (d · 5) (mod 6) = 1. Drugim riječima tražimo višekratnik broja 5 koji pri dijeljenju s 6 daje ostatak 1. Postoji više rješenja, npr. d = 5, 11, 17, itd. Tada je privatni ključ uređeni par (d, n), tj. (5,14), (11,14), (17,14), itd. Kad odredimo javni i privatni ključ slijedi postupak šifriranja i dešifriranja. Napišimo još jednom ključeve: javni ključ (5,14) i privatni ključ npr. (11,14). Recimo da želimo poslati numeričku poruku x = 2. Koristimo javni ključ i računamo y = x e (mod 14) tj. y = 25 (mod 14) = 4. Šifrirana poruka glasi y = 4. Da bi dešifrirali poruku koristimo privatni ključ i računamo x = y d (mod 14) tj. x = 411 (mod 14) = 2 i time smo dobili polaznu poruku.
Aktivnost: Izrada ključeva (25 min)

Opis aktivnosti: Svaki učenik izrađuje vlastiti par ključeva, šifrira brojčanu poruku i šalje je drugom učeniku, prima i dešifrira poruku.
Aktivnost: Šifriranje i dešifriranje poruka (20 min)

Opis aktivnosti: Učenici koriste Python naredbu pow(12,73,589) i istražuju kako računalo vrlo brzo računa velike potencije s ostatkom.
Aktivnost: Dodatni zadatak (15 min)

Opis aktivnosti: Učenici uočavaju da se dijeljenje s ostatkom, koje uče u školi, koristi u suvremenim tehnologijama za zaštitu podataka, internetsko bankarstvo, mobilne aplikacije i sigurnu komunikaciju.
Aktivnost: Završni dio (5 min)