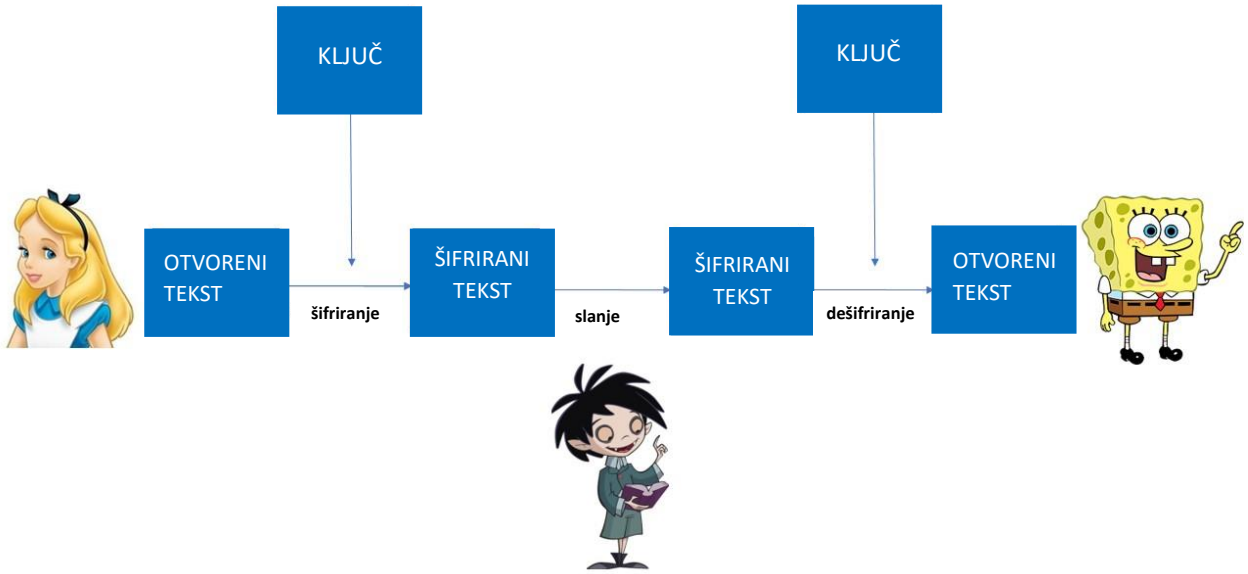
KRIPTOGRAFIJA (ŠIFRIRANJE)

Šifriranje je proces izmjene originalnog teksta u šifrirani tekst pomoću određenog ključa. Obrnuti proces, dešifriranje, omogućava onome kome je poznat ključ da pročita šifriranu poruku.



Otkada je civilizacije, postoji potreba za šifriranje. Spartanci su za šifriranje koristili skital: štap oko kojeg je namotana vrpca od pergamenta na koju su zapisali tajnu poruku. U ovom primjeru ključ je debljina štapa: svatko tko je imao štap iste debljine mogao je pročitati poruku.

CEZAROVA ŠIFRA

Gaj Julije cezar je šifrirao tako da je svako slovo u poruci zamijenio slovom koje je tri mjesta nakon njega u abecedi (A je zamijenio s D, B sa E, itd.). Za šifrirati Cezarovom šifrom, možemo koristiti Cezarov disk: slova u vanjskom (gornjem) krugu zamijenimo odgovarajućim slovima u unutarnjem (donjem) krugu.

Iako je Cezar bio veliki vojskovođa, nije bio vrsan matematičar: njegovu šifru možemo probiti u najviše 26 pokušaja. Danas, u čast Cezaru, Cezarovom šifrom zovemo ovakvu metodu šifriranja gdje je pomak određen bilo kojim brojem manjim od 25. U ovom primjeru šifriranja ključ je broj koji određuje za koliko mjesta pomičemo svako slovo.

ENIGMA

Enigma strojevi su serija elektromehaničkih rotorskih strojeva za šifriranje, uglavnom razvijenih i korištenih početkom do sredine 20. stoljeća za zaštitu komercijalne, diplomatske i vojne komunikacije. Enigmu je izumio njemački inženjer Arthur Scherbius na kraju Drugog svjetskog rata. Alan Turing, matematičar i logičar sa Sveučilišta Cambridge, pružio je veći dio originalnog razmišljanja koje je na kraju dovelo do razbijanja Enigme sredinom 20. stoljeća.

UPUTE ZA KORIŠTENJE ENIGME:

1. Definirajte inicijalni redoslijed zupčanika.
2. Definirajte inicijalni ključ koji se sastoji od 3 slova. Nakon određivanja redoslijeda zupčanika, ključ određuje njihovu orijentaciju.
3. Napišite tekst koji želite šifrirati. Nemojte koristiti razmak niti interpunkcijske znakove.
   Zupčanik s desne strane je zupčanik na koji namještamo znakove otvorenog teksta kojeg želimo šifrirati. Za početak šifriranja pronađite prvo slovo svoje poruke i poravnajte ga sa strelicom pored ovog zupčanika. Pročitajte odgovarajuće slovo koje se pojavljuje na gornjoj strelici zupčanika 1 (lijevi zupčanik na ploči). Napišite ovo slovo odmah ispod slova koje ste upravo šifrirali. Zatim postavite prvi zupčanik na drugo slovo vaše poruke. Pročitajte kodirano slovo na 2. (srednjem) zupčaniku. Ponovite postupak sve dok ne iscrpite sva slova otvorenog teksta.

VIZUALNA KRIPTOGRAFIJA

Kako sakriti sliku? Je li moguće podijeliti tajnu grupi prijatelja tako da svaki dobije samo dio informacije, a tajna poruka bude vidljiva samo kada se određeni broj dijelova spoji?

Vizualna kriptografija (vizualno šifiriranje) je metoda podijele slike na određeni broj dijelova tako da svaki dio sam za sebe ne nosi nikakvu informaciju. Vizualno šifriranje su uveli Adi Shamir i Moni Naor u 1994., nakon čega je počeo rasti interes za ovom metodom šifriranja.

ŠIFRIRANJE JAVNIM KLJUČEM

Prilikom šifriranja javnim kljulem, Alice ima par ključeva: javni ključ E_{Alice} pomoću kojega ostali šifriraju njoj namijenjene poruke i tajni ključ D_{Alice} koji ona koristi za čitanje primljenih (šifriranih) poruka. Javni ključ je dostupan svima, a tajni ključ samo vlasniku. Možemo zamisliti javni i tajni ključ kao sandučić s lokotom i ključićem: svaka osoba ima svoj sandučić s lokotom i pripadni ključić koji otvara lokot. Sandučić s lokotom je dostupan svima i svatko može "zaključati" poruku, ali samo osoba koja ima ključić poruku može pročitati. Na primjer, kada Bob želi poslati poruku Alice, on poruku spremi u Alicein sandučić i zaključa ju njezinim lokotom. Samo Alice ima ključić svog lokota i samo ona može otključati poruku namijenjenu njoj.

Danas se šifriranje javnim ključem temelji na procedurama baziranim na NP-teškim matematičkim problemima.

UPUTE ZA MICRO:BIT

Micro:bit za šifriranje

(i) Tipka B: odaberi javni ključ osobe kojoj želiš poslati poruku
(ii) Tipka A: odaberi slovo koje želiš šifrirati
(iii) Tipke A i B istovremeno: šifrira se odabrano slovo
(iv) Ponavljaj korake (ii) i (iii) dok nisi šifrirao/šifrirala sva slova poruke koju želiš poslati

Micro:bit za dešifriranje

(i) Tipka B: odaberi svoj tajni ključ
(ii) Tipka A: odaberi slovo koje želiš dešifrirati
(iii) Tipke A i B istovremeno: dešifrira se odabrano slovo
(iv) Ponavljaj korake (ii) i (iii) dok nisi dešifrirao/dešifrirala sva slova šifirirane poruke