Simetrično šifrovanje i dešifrovanje

Simetrično šifrovanje

• Konvencionalno / sa tajnim ključem / sa jednim ključem

• Pošiljalac i primalac dele zajedni čki ključ

• Svi klasi čni algoritmi šifrovanja su zasnovani na tajnom ključu

• Jedini tip šifrovanja do otkri ća javnih klju čeva u sedamdesetim godinama prošlog veka 2/52

Osnovna terminologija

• plaintext otvoreni tekst - originalna poruka

• ciphertext šifrovana poruka – kodirana poruka

• cipher šifra – algoritam transformacije originalne u kodiranu poruku

• key klju č – informacija koriš ćena u šifri, poznata samo pošiljaocu/primaocu

• encipher (encrypt) šifrovanje (kriptovanje) – konverzija originalne poruke u kodiranu

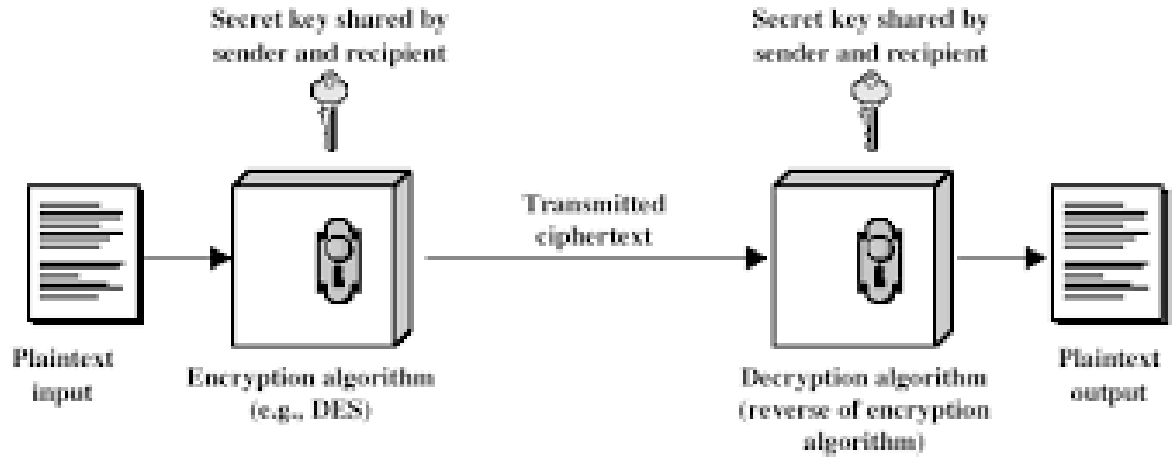
• decipher (decrypt) dešifrovanje (dekriptovanje) – obnavljanje originalne poruke iz kodirane

• cryptography kriptografija – nauka o metodama i principima šifrovanja

• cryptanalysis (codebreaking) kriptoanaliza (razbijanje šifre) – nauka o metodama i principima dešifrovanja šifrovane poruke bez poznavanja klju č a

• cryptology kriptologija – kriptografija + kriptoanaliza

Model simetričnog šifrovanja



Kao što smo rekli, kod simetrične enkripcije koriste se isti ključ i za šifrovanje i za dešifrovanje. Baš zbog toga je raznovrsnost, a samim tim i sigurnost algoritama ovakve enkripcije je velika. Bitan faktor je i brzina - simetrična enkripcija je veoma brza.

Pored svih prednosti koje ima na polju sigurnosti i brzine algoritma, postoji i jedan veliki nedostatak. Kako preneti tajni ključ? Problem je u tome, što ako se tajni ključ presretne, poruka se može pročitati.

Zato se ovaj tip enkripcije najčešće koristi prilikom zaštite podataka koje ne delimo sa drugima (šifru znate samo vi i nju nije potrebno slati drugome).

Klod Šenon (Claude Shannon) je definisao uslove savršene tajnosti, polazeći od sledećih osnovnih pretpostavki:

1. Tajni ključ se koristi samo jednom.
2. Kriptoanalitičar ima pristup samo kriptogramu.

Šifarski sistem ispunjava uslove savršene tajnosti ako je otvoreni tekst X statistički nezavisan od kriptograma Y, što se može matematički izraziti na sledeći način:

$$P(X = x|Y = y) = P(X = x)$$

za sve moguće otvorene tekstove i sve moguće kriptograme ;

drugim rečima, verovatnoća da slučajna promenljiva X ima vrednost x jednaka je sa ili bez poznavanja vrednosti slučajne promenljive Y.

Zbog toga kriptoanalitičar ne može bolje proceniti vrednost X poznavajući vrednost Y od procene bez njenog poznavanja, nezavisno od raspoloživog vremena i računarskih resursa kojima raspolaže.

Koristeći pojam entropije iz teorije informacija, Šenon je odredio minimalnu veličinu ključa potrebnu da bi bili ispunjeni uslovi savršene tajnosti. dužina ključa K mora biti najmanje jednaka dužini otvorenog teksta M:

$$K \geq M$$

Literatura:

https://rti.etf.bg.ac.rs/rti/ ir4zp/materijali/predavanja/2018/02%20Simetricno%20sifrovanje.pdf

https://sh.wikipedia.org/wiki/Kriptografija