Simetrični algoritmi zaštite

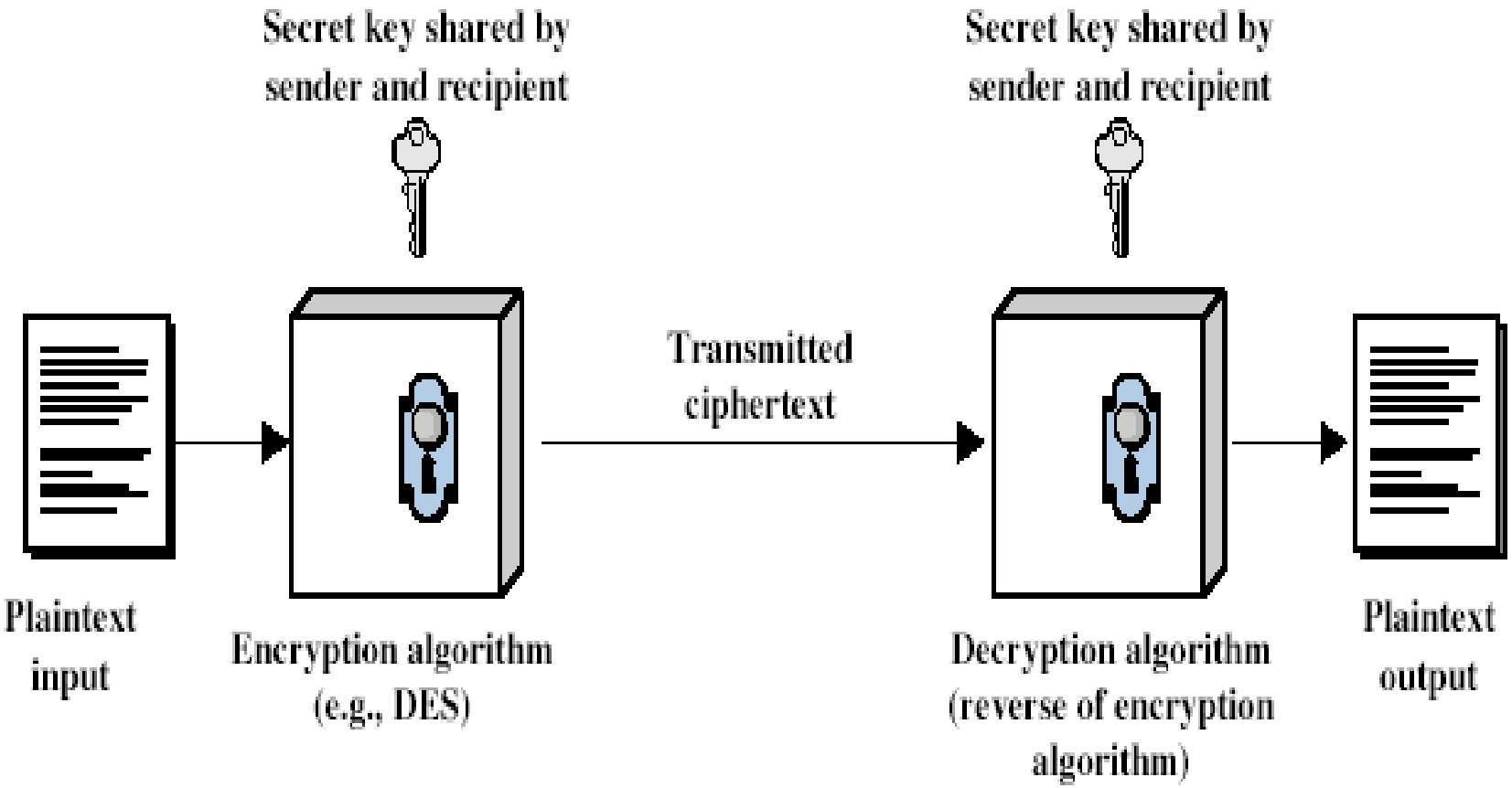
Kriptovanje (Šifrovanje)
Simetrično šifrovanje

- Konvencionalno / sa tajnim ključem / sa jednim ključem
- Pošiljalac i primalac dele zajednički ključ
- Svi klasični algoritmi šifrovanja su zasnovani na tajnom ključu
- Jedini tip šifrovanja do otkrića javnih ključeva u sedamdesetim godinama prošlog veka

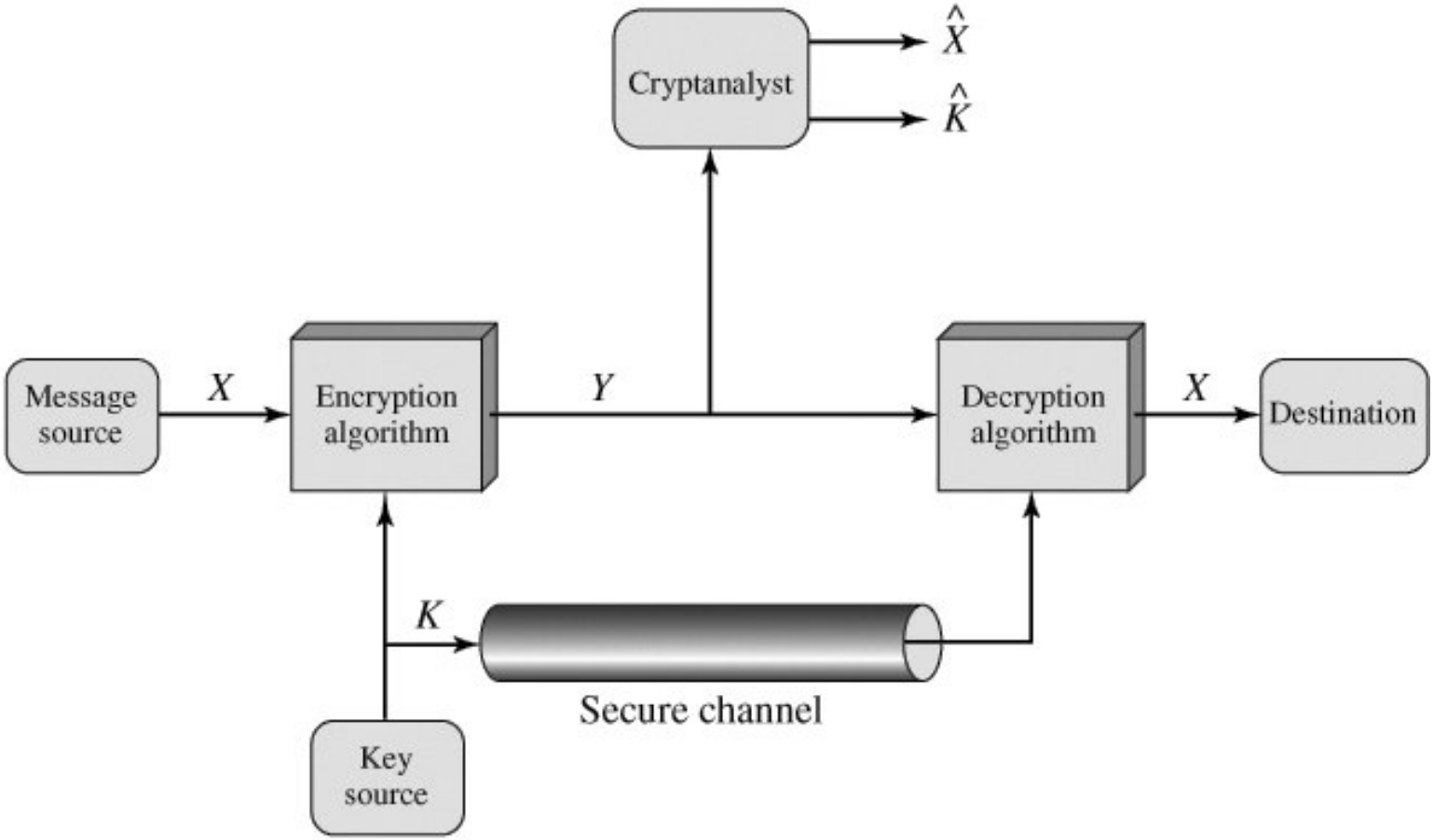
Osnovna terminologija

- **plaintext *otvoreni tekst*** - originalna poruka
- **ciphertext *šifrovana poruka*** – kodirana poruka
- **cipher *šifra*** – algoritam transformacije originalne u kodiranu poruku
- **key *ključ*** – informacija korišćena 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 ključa
- **cryptology *kriptologija*** – kriptografija + kriptoanaliza

Model simetričnog šifrovanja



Model kriptosistema



Zahtevi

- Dva zahteva za sigurnu upotrebu simetričnog šifrovanja:
  - Jak algoritam šifrovanja (čak i kada je poznat veći broj šifrovanih tekstova i njihovih otvorenih poruka, nije moguće dešifrovati novi šifrovani tekst)
  - Tajni ključ poznat samo pošiljaocu i primaocu

    $Y = E_K(X)$

    $X = D_K(Y)$
- Pretpostavlja se da je algoritam šifrovanja poznat
- Podrazumeva siguran kanal za distribuciju ključa

Kriptografija

- Određeno je:
  - Tipom korišćene operacije šifrovanja
    - Supstitucija / transpozicija / proizvod - ponavljanje
  - Brojem ključeva
    - Jedan ključ ili tajna / dva ključa ili javna
  - Načinom na koji se obrađuje originalni tekst
    - Block ***(blokovski)*** / stream ***(u toku ili sekvencijalno)***

Tipovi napada u kriptoanalizi

- **Poznata samo kodirana poruka**
  - Poznati samo algoritam, kodiran tekst i statistika i može da identifikuje originalan tekst
- **Poznat originalan tekst**
  - Poznati ili pretpostavljeni originalan tekst i kodirani tekst.
- **Izabran originalni tekst**
  - Izabere se originalan tekst da se dobije kodirani
- **Izabran kodirani tekst**
  - Izabran kodirani tekst da se dobije originalna
- **Izabrani tekst**
  - Izabere bilo originalni ili kodirani tekst

Napad grubom silom

- Proba se svaki ključ
- Osnovni napad, trajanje razbijanja proporcionalno dužini ključa
- Pretpostavlja se bilo poznat ili prepoznatljiv originalan tekst

Key Size (bits)	Number of Alternative Keys	Time required at 1 encryption/μs	Time required at 10^6 encryptions/μs
32	$2^{32} = 4.3 \times 10^9$	$2^{31}\ \mu s = 35.8$ minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55}\ \mu s = 1142$ years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127}\ \mu s = 5.4 \times 10^{24}$ years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167}\ \mu s = 5.9 \times 10^{36}$ years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26}\ \mu s = 6.4 \times 10^{12}$ years	6.4×10^{6} years

Dodatne definicije

- **Bezuslovna sigurnost**
  - Bez obzira na raspoložive računare, šifra se ne može razbiti, jer kodirana poruka nema dovoljno informacije da jedinstveno odredi odgovarajući originalan tekst
- **Računarska sigurnost**
  - Pri datim računarskim resursima, šifra se ne može razbiti u smislenom vremenu

Klasične supstitucione šifre

- Slova originalnog teksta se zamenjuju drugim slovima, brojevima ili simbolima
- Ako se originalan tekst posmatra kao niz bita, supstitucija obuhvata zamenu grupe bita originalnog teksta sa grupom bita kodiranog teksta

Radio: Ilija Paunovic