Cryptanalysis and its Types | What is Cryptology in Network Security

1.75
1:35 / 10:02

CRYPTANALYSIS and CRYPTOLOGY

In simple words, cryptanalysis is a technique of decoding messages from a non-readable format → readable format without knowing the key.

or $P.T\ \square \rightarrow \square$ cipher □

we can sa it is the science of recovering the plainte of the message without having access to t key.

More techn definition can be,

Cryptanal used to break cryptographic security gain access to the messages, even if contents ysis is a technique of decoding messages from a non-readable format → readable format without knowing the key.

P.T □ → □ cipher □

or

we can say it is the science of recovering the plaintext of the message without having access to the key.

More technical definition can be,

Cryptanalysis is used to break cryptographic security systems and gain access to the contents of the encrypted messages, even if cryptographic key is unknown.

There are various cryptanalytic attacks

(i) Ciphertext only attack

knows only ciphertext.

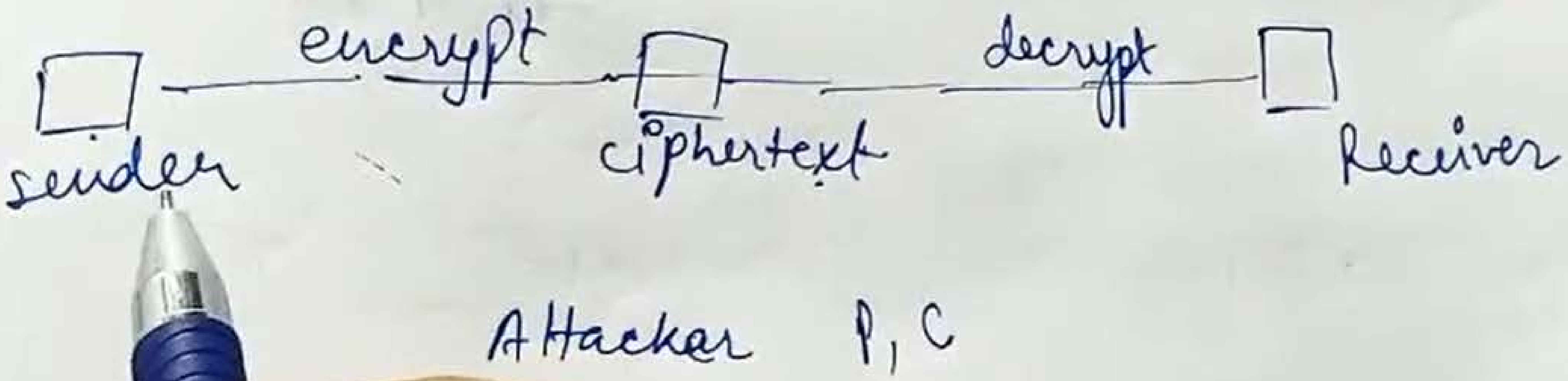
can be,

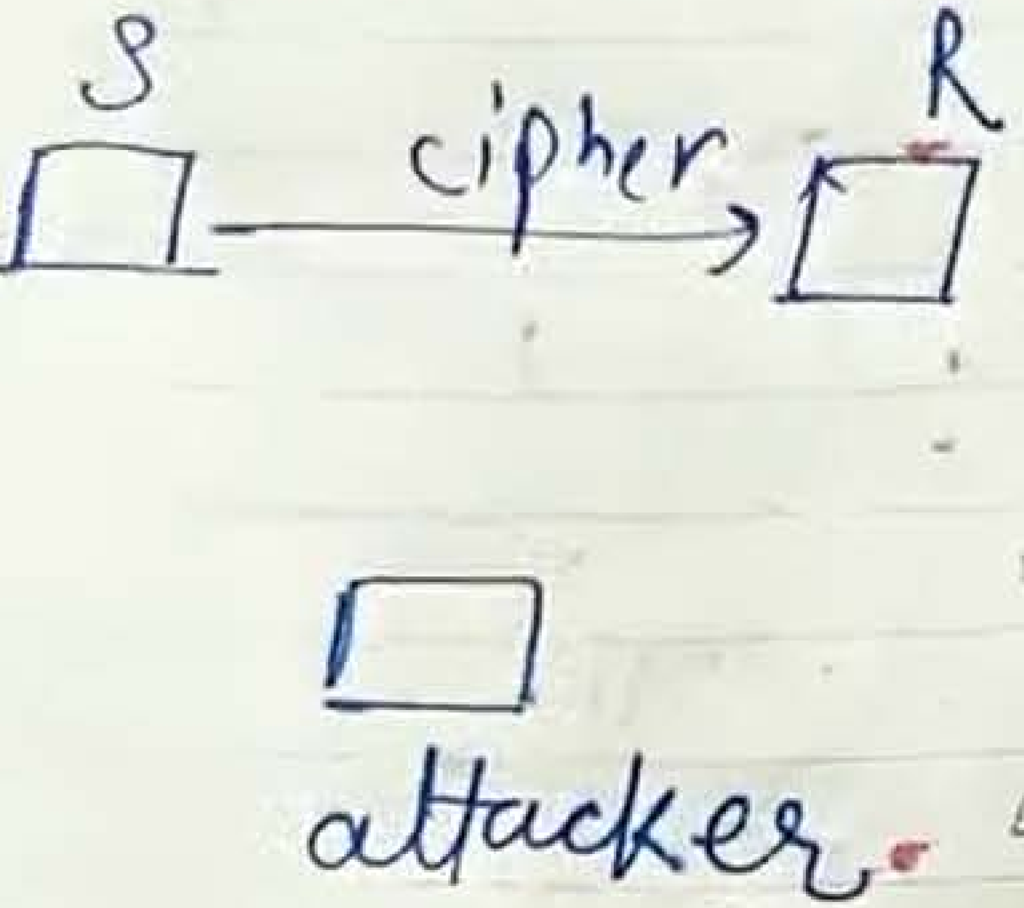
Cryptanalysis is used to break cryptographic security systems and gain access to the contents of the encrypted messages, even if cryptographic key is unknown.

There are various cryptanalytic attacks

(i) Ciphertext only attack
attacker knows only ciphertext.

(ii) Known plaintext only attack
attacker knows some combination of Pi, Ci and based on these, he try to decrypt the messages.





(iii) chosen plaintext attack

model of cryptanalysis which assumes that the attacker can choose random plaintexts to be encrypted and obtain the corresponding ciphertexts.

The goal of attacker is to gain further info. which reduces the security of the encryption scheme.

In the worst case, this attack can expose the secret information after calculating the secret key

(iv) Chosen ciphertext attack

attacker ~~chooses~~ can analyze any ciphertext C_i and gets thei corresponding decryptions - plaintexts P_i.

1.75
7:27 / 10:02
Receiver
cipher
der
rx4#$
Attacker
paper
book

Cryptanalysis and its Types | What is Cryptology in Network Security

the worst case, this attack can expose the secret information after calculating the secret key.

(iv) Chosen Ciphertext attack

attacker ~~chooses~~ can analyze any ciphertext C_i and gets their corresponding decryptions - plaintexts P_i.

His goal is to acquire a secret key or to get as many info. about the attacked system as possible.

The attacker has capability to make the victim decrypt any ciphertext and send him back the result.

s, by analyzing the chosen ciphertext a

plaintext, the int

ElGamal Cryptography: Asymmetric Key.

i) Key Generation:

i) Select Large Prime no. (P) ⇒ P = 11

ii) Select decryption Key / Private Key (D) = 3

iii) Select second part of encryption key or public key (E1) = 2

iv) Third part of the encryption Key or public key (E2). $E2 = \underline{E1^D \bmod P} \Rightarrow 8$

v) Public Key = (E1, E2, P), Private key = D

⇒ (2, 8, 11) , ↳ 3

$(125)^{-1} \bmod 11$

$(125 \times x) \bmod 11 = 1$

$\boxed{x = 3,}$

ii) Encryption:

i) Select Random Integer (R) ⇒ 4

ii) $C1 = E1^R \bmod P$, $C1 = 2^4 \bmod 11 = 5$

iii) $C2 = (PT \times E2^R) \bmod P = (7 \times 8^4) \bmod 11$

$\Rightarrow 28672 \bmod 11$

$\Rightarrow 6$

iv) C.T = (C1, C2)

iii) Decryption:

$PT = [C2 \times (C1^D)^{-1}] \bmod P$

$P = 11, D = 3, E1 = 2 \;\Big\}\; \boxed{P.T = 7}$

$E2 = (2)^3 \bmod 11 = 8 \bmod 11 = \textcircled{8}$

$C1 = 5, \quad C2 = 6$

$\textcircled{7} \xrightarrow[\uparrow\ \text{Encryption.}]{} \boxed{C.T = (5,6)} \xrightarrow[\text{Decryption}\ \downarrow]{} \boxed{P.T = 7}$

$P.T = (6 \times (5^3)^{-1}) \bmod 11$

$\Rightarrow (5^3)^{-1} \bmod 11 \Rightarrow 3$

$(6 \times 3) \bmod 11 \Rightarrow 18 \bmod 11$

$\boxed{P.T = 7}$