[CS304] Introduction to Cryptography and Network Security

Course Instructor: Dr. Dibyendu Roy | Winter 2022-2023
Scribed by : Pallikonda Sai Teja | Lecture (Week 04)
Student ID : 202011052

1 Attack Model

1.1 Cipher Text only Attack

Attacker knows only cipher text.
Goal : Recover the plain text corresponding to the cipher text or recover the secret key.

1.2 Known Plain Text Attack

Attacker knows some plain text and corresponding cipher texts.
Goal : Generate new plain text, cipher text pair or recover the secret key.

1.3 Chosen Plain Text Attack

Attacker chooses plain text according to his/her choice and (s)he will be provided the corresponding cipher text.
Goal : Generate new plain text, cipher text pair or recover the secret key.

1.4 Chosen Cipher Text Attack

Attacker chooses some cipher text and he/she is allowed to get the corresponding plain text.
Goal : Generate a new plain text and cipher text pair or recover the secret key.

*** DES(M,K) = C**
*** DES**(M^c, K^c) = C^c
Key = 56 bit Brute Force/Exhaustive search = 2^{56}

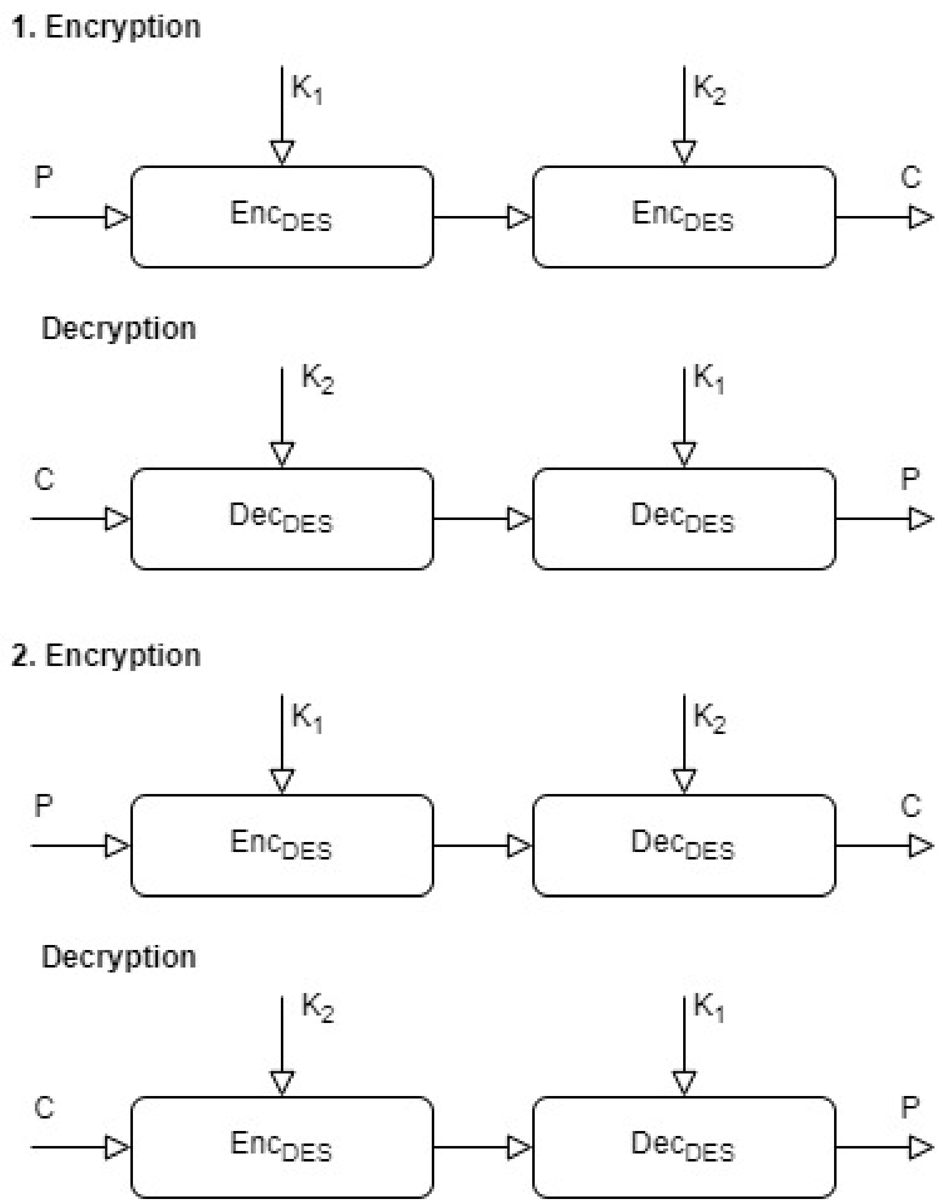
1.5 Chosen Plain Text Attack on DES

⇒ Attacker chooses two plain texts.
I) M, II) M^c
Challenge is to find key K
c_1 = DES(M,K)
c_2 = DES(M^c,K)
Attacker is getting c_1 and c_2.
DES($(M^c)^c, k^c$) = DES(M, k^c) = ${c_2}^c$
Keys = {K_1,k_2,k_3,...,$K_{2^{56}}$}
Attacker selects k_1 ∈ Keys. He also know that ${k_1}^c$ ∈ Keys.
Attacker preforms DES(M,K_1) = $\widetilde{c}$
if $\widetilde{c} \neq c_1$ or $\widetilde{c} \neq c_2$
then discard K_1,${K_2}^c$ (why?)

if $\widetilde{c} \neq \mathrm{c}_1 \Rightarrow \mathrm{K}_1 \neq \mathrm{K}$
if $\widetilde{c} \neq {c_2}^c \Rightarrow \mathrm{K}_1 \neq K^c \Rightarrow {K_1}^c \neq \mathrm{K}$
In every search attacker is eliminating two keys. So, search $= \frac{2^{56}}{2} = 2^{55}$
* DES $\rightarrow$ is not secure due to multiple attacks.
So, Increase the length of the secret key.

1.6 Double Encryption

$\mathrm{K} = \mathrm{K}_1 \parallel \mathrm{K}_2$
$\mathrm{len}(\mathrm{K}_1) = 56$ bit, $\mathrm{len}(\mathrm{K}_2) = 56$ bit $\}$ $\mathrm{len}(\mathrm{K}) = 112$ bit

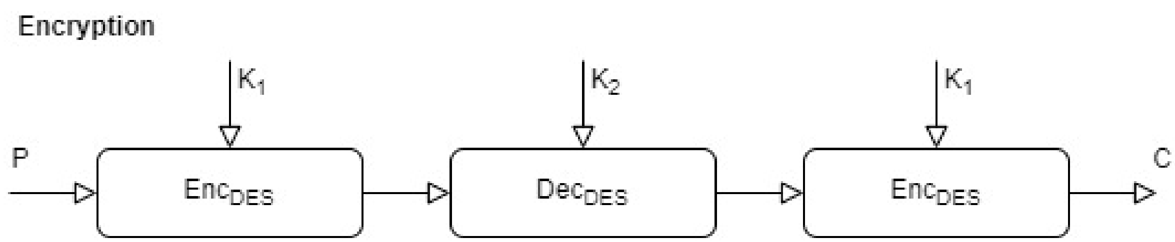


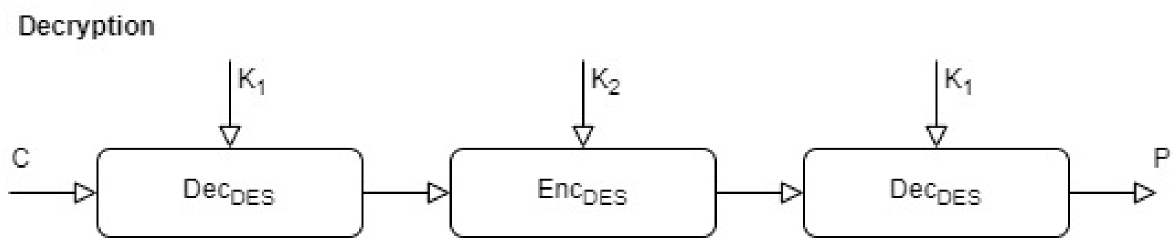
* EE, ED, DE, DD.
$\mathrm{K} = \mathrm{K}_1 \parallel \mathrm{K}_2$

Attacker knows plain text M and the corresponding ciphet text c.
c = Enc(Enc(M,K_1),K_2)
Keys = $\{SK_1, SK_2, SK_3, \ldots, SK_{2^{56}}\}$
Enc(M, SK_i) = X_i
Dec(C, SK_j) = Y_j
if $X_i = Y_j$ for some i,j then the key is $SK_i \| SK_j$

1.7 Triple Encryption

$K = K_1 \| K_2$ 2n-bit Encryption





* EEE, EDE, DED,...

2 Advanced Encryption Standard AES

→ We have to understand certain mathematical results.
⇒ A binary operation * on a set S is a mapping from S x S to S.
That is * is a rule which assigns to each ordered pair of elements from S to an element of S.

$$* : SxS \to S$$

*(a,b) = c
*(b,a) = d a,b,c,d $\in$ S
It is not necessary that d = c.

2.1 Group

A Group (G,*) consists of a set G with a binary operation * on G satisfing the following axioms.

1. * is associative on G
   a*(b*c) = (a*b)*c $\forall$ a,b,c $\in$ G
2. There is an element e $\in$ G called the identity element such
   a*e = a = e*a $\forall$ a $\in$ G

3. For each a ∈ G there exists an element a^{-1} ∈ G called the inverse of a such that a*a^{-1} = e = a^{-1}*a ∀ a ∈ G

* A Group G is called abelian (or commutative) if

$$a * b = b * a \; \forall \; a, b \in G$$

Example 01: * : Matrix multiplication over square matrices of order n x n
M : set of n x n matrices over R
(M,*) → it is not a Group.

1. * is associative on M
$$A * (B * C) = (A * B) * C$$
2. A * I_n = A = I_n * A
3. ∀ A ∈ M there may not exists A^{-1} ∈ M such that
$$A * A^{-1} = I_n = A^{-1} * A$$

⇒ M = {Set of all invertable matrices n x n matrix }
(M,*) → Group.
(M,*) is not commutative since A * B ≠ B * A

Example 02: Z : Set of all integers $(Z, +)$ is a Group

1. + is associative on Z
$$a + (b + c) = (a + b) + c$$
2. a + 0 = a = 0 + a, ∀ a ∈ Z
3. ∀ a ∈ Z there exists -a ∈ Z such that
$$a + (-a) = 0 = (-a) + a$$

Example 03: Z : Set of all integers $(Z, *)$ is not a Group

1. * is associative on Z
$$a * (b * c) = (a * b) * c$$
2. a * 1 = a = 1 * a, ∀ a ∈ $\{Z - \{0\}\}$
3. ∀ a ∈ Z there does not exists b ∈ Z such that
$$a * b = 1 = b * a$$

Example 04: Q : Set of all rational numbers
$(Q, *)$ is not a Group
$(Q - \{0\}, *)$ is Group

1. * is associative on Q
$$a * (b * c) = (a * b) * c$$

2. a * 1 = a = 1 * a, $\forall$ a $\in \{Q - \{0\}\}$

3. $\forall$ a $\in \{Q - \{0\}\}$ there exists b $\in \{Q - \{0\}\}$ such that

$$a * b = 1 = b * a$$

* If |G| is finite then (G,*) is finite group.
|G| : Cardinality of G.
Example 05:$(Z_{\mathrm{n}}, +_{\mathrm{n}}) \rightarrow$ Group. Z_{n} = {0,1,2,..,n-1}
x $+_{\mathrm{n}}$ y = (x + y)mod n

1. $+_{\mathrm{n}}$ is associative on Z_{n}
$$a +_{\mathrm{n}} (b +_{\mathrm{n}} c) = (a +_{\mathrm{n}} b) +_{\mathrm{n}} c$$

2. a $+_{\mathrm{n}}$ 0 = a = 0 $+_{\mathrm{n}}$ a, $\forall$ a $\in Z_{\mathrm{n}}$

3. $\forall$ a $\in Z_{\mathrm{n}}$ there exists (n-x) $\in$ $\mathrm{Z_n}$ such that

$$a +_{\mathrm{n}} (n - a) = 0 = (n - a) +_{\mathrm{n}} a$$

4. $(Z_{\mathrm{n}}, +_{\mathrm{n}})$ is commutative
$$a +_{\mathrm{n}} b = b +_{\mathrm{n}} a$$

Example 06:$(Z_{\mathrm{n}} - \{0\}, *_{\mathrm{n}})$
x $*_{\mathrm{n}}$ y = (x * y)mod n $*_{\mathrm{n}}$: multiplication modulo n.

1. $*_{\mathrm{n}}$ is associative on Z_{n}
$$a *_{\mathrm{n}} (b *_{\mathrm{n}} c) = (a *_{\mathrm{n}} b) *_{\mathrm{n}} c$$

2. a $*_{\mathrm{n}}$ 1 = a = 1 $*_{\mathrm{n}}$ a, $\forall$ a $\in Z_{\mathrm{n}} - \{0\}$

3. a $*_{\mathrm{n}}$ b = b $*_{\mathrm{n}}$ a $\forall$ a = 1 such that
   a $*_{\mathrm{n}}$ b = 1
   $\Rightarrow$ a.b = 1 + t.n
   $\Rightarrow$ 1 = a.b + t_1.n
   $\Rightarrow$ gcd(a, n) = 1

* Z^* = {x | gcd(x, n) = 1}
$\Rightarrow$ (Z^*, $*_{\mathrm{n}}$) $\rightarrow$ group.
$|Z^*| = \phi$(n)
ϕ(n) is Euler's totient function