[CS304] Introduction to Cryptography and Network Security

Course Instructor: Dr. Dibyendu Roy
Scribed by: Akshay (202051018)

Winter 2022-2023
Lecture (Week 4)

1 Attack Models

1.1 Cipher-text only Attack

Attackers Knows only ciphertexts.
Goal:- Recover the plaintexts corresponding to the ciphertexts or recover the secret key.

1.2 Known Plaintext Attack

Attacker knows some plaintexts and corresponding ciphertexts.

1.3 Chosen Plaintext Attack

Attackers chooses plaintexts according to hi/her choice and (s)he will be provided the corresponding ciphertexts.
Goal:- Generate new plaintext, ciphertext pair or recover the secret key.

1.4 Chosen Ciphertext Attack

Attacker chooses some ciphertext and he/she is allowed to get the corresponding plaintexts.
Goal:- Generate a new plaintext and ciphertext pair or recover the secret key.

Order of strongness of above attacks:
$1 < 2 < 3 < 4$

2

$$DES(M, K) = C$$
$$DES(\overline{M}, \overline{K}) = \overline{C}$$

Key = 56; Brute force attack/Exhaustive search = 2^{56}

Attacker chooses two plaintexts:
1) M 2) $\overline{M}$
Provided by corresponding ciphers C_1 and C_2, both encrypted with the same key.

$$C_1 = DES(M, K)$$

$$C_2 = DES(\overline{M}, K)$$

Challenge is find the key K (CPA, Chosen plaintext attack).

From the design of DES:

$$DES(\overline{\overline{M}}, \overline{K}) = \overline{C_2}$$
$$\implies DES(M, \overline{K}) = \overline{C_2}$$
$$\text{Keys} = \{K_1, K_2, ..., K_{2^{56}}$$

Attacker selects $K_1 \in$ Keys.
He knows that $\overline{K_1} \in$ Keys.

Attacker performs $DES(M, K_1) = C$
If $\tilde{C} \neq C_1$ or $\tilde{C} \neq \overline{C_2}$
then discard K_1 and $\overline{K_1}$

Because:
$\tilde{C} \neq C_1 \implies K_1 = K$
$\tilde{C} \neq \overline{C_2} \implies K_1 \neq \overline{K} \implies \overline{K_1} \neq K$

Search space is reduced to half

DES is not secure due to multiple attacks.

3 Making DES Secure from Attacks

Increase the length of the secret key.

3.1 Idea of Double Encryption

$$K = K_1 || K_2$$

length of $K_1 = 56$ bit
length of $K_2 = 56$ bit
$\implies$ len(K) = 112 bit

1) Enc:

$$\text{P} \rightarrow \overset{\downarrow K_1}{\boxed{Enc_{DES}}} \rightarrow \overset{\downarrow K_2}{\boxed{Enc_{DES}}} \rightarrow \text{C}$$

Dec:

$$\text{C} \rightarrow \overset{\downarrow K_2}{\boxed{Dec_{DES}}} \rightarrow \overset{\downarrow K_1}{\boxed{Dec_{DES}}} \rightarrow \text{P}$$

2) Enc:

$$\text{P} \rightarrow \overset{\downarrow K_1}{\boxed{Enc_{DES}}} \rightarrow \overset{\downarrow K_2}{\boxed{Dec_{DES}}} \rightarrow \text{C}$$

Dec:

$$\text{C} \rightarrow \overset{\downarrow K_2}{\boxed{Enc_{DES}}} \rightarrow \overset{\downarrow K_1}{\boxed{Dec_{DES}}} \rightarrow \text{P}$$

- EE, ED, DE, DD

This Idea of doing double encryption does not provide any extra security
Proof:
$K = K_1||K_2$
Attacker knows plaintext M and the corresponding ciphertext C.

$$C = Enc(Enc(M, K_1), K_2)$$

Keys $= \{SK_1, ..., SK_{2^{56}}\}$ (We have to select K_1 and K_2 from the same set of 2^{56} keys.
$Enc(M, SK_i) = X_i$
$Dec(C, SK_j) = Y_j$
If $X_i = Y_j$ then $SK_i = K_1$ and $SK_j = K_2$
Time complexity is still 2^{56} instead of 2^{112}
Hence, encrypting twice does not provide any extra security. It is true for all algorithms.

3.2 Triple Encryption

$K = K_1||K_2$; 2n-bit security

1) Enc:

$$\text{P} \rightarrow \overset{\downarrow K_1}{\boxed{Enc}} \rightarrow \overset{\downarrow K_2}{\boxed{Dec}} \rightarrow \overset{\downarrow K_1}{\boxed{Enc}} \rightarrow \text{C}$$

Dec:

$$\text{C} \rightarrow \overset{\downarrow K_1}{\boxed{Dec}} \rightarrow \overset{\downarrow K_2}{\boxed{Enc}} \rightarrow \overset{\downarrow K_1}{\boxed{Dec}} \rightarrow \text{P}$$

- EEE, EDE, DED, ...

If DES is used in Triple encryption setup then it is known as Triple DES (3-DES)

4 Maths Pre-requisite for AES

We have to understand certain mathematical results.

4.1 Binary Operation

A binary operation $\star$ on a set S is a mapping from S×S to S.
That is $\star$ is a rule which assigns to each ordered pair of elements from S to an element of S.
$\star : S \times S \rightarrow S$
$\star(a, b) = c$, a,b,c $\in$ S

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

4.2 Group

A group (G, $\star$) consists of a set G with a binary operation $\star$ on G satisfying the following axioms.

1. $\star$ is associative on G.
   $a \star (b \star c) = (a \star b) \star c \ \ \forall$ a,b,c $\in$ G.
2. There is an element e $\in$ G called the identity element such that:
   $a \star e = a = e \star a \ \ \forall$ a $\in$ G.
3. For each $a \in G$ there exists an element $a^{-1} \in G$ called the inverse of 'a' s.t. $a \star a^{-1} = e = a^{-1} \star a$
   $\forall$ a $\in$ G.

A group G is called abelian (or commutative) if:
$a \star b = b \star a \ \ \forall$ a,b $\in$ G.

Example:
1)
$\star$: matrix multiplication over square matrices of order nn
M : set of $n \times n$ matrices over $\mathbb{R}$
(M, $\star$) - Is it a Group? Ans: No, because all square matrices are not invertible.

2)
$\mathbb{Z}$: set of all integers.
$(\mathbb{Z}, +)$: Is it a group? Ans: Yes

1. a+(b+c) = (a+b)+c
2. a + 0 = a = 0 + a $\qquad \forall$ a $\in$ Z
3. $\forall$ a $\in \mathbb{Z} \ \ \exists$ -a $\in \mathbb{Z}$ s.t. a + (-a) = 0 = (-a) + a

3)
$\mathbb{Z}$: set of all integers
$(\mathbb{Z}, +)$: Group? Ans: Yes

4)
$(\mathbb{Z}, \times)$: Not a group.
$a \in \mathbb{Z} \ \nexists \ a^{-1} \in \mathbb{Z}$

5)
Q : set of all rational numbers.
(Q, $\times$) : Not a group
(Q - {0}, $\times$) : group

If $|G|$ is finite then (G, $\times$) is a finite group.
$|G|$: Cardinality of G

Example:
$Z_n = \{0, 1, ..., n-1\}$
$(Z_n, +_n)$: group
$x +_n y = (x + y) mod\ n$

$(Z_n - \{0\}, \times_n)$: not a group because not all numbers have inverse under modulo n.