22-02-22

CSPC63 – Principle of Crypto.

106119100
Rajneesh

Crypto – CT 1

Question (1):

In crypto attack the aim of the attacker is to break the secrecy of the encryption and learn the secret message and even better, the secret key.

Types of attacks:

(1) Brute-force-Attack:

Simple Attack on cipher is the brute force attack. In this, an attacker simply tries to decrypt the message with each possible secret key and checks the result of decryption to see if its correct.

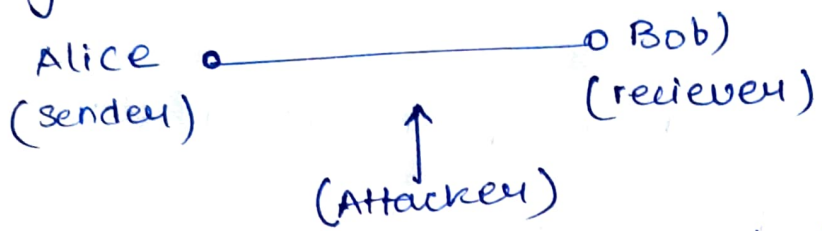
for eg.
longest available key length of of AES cipher is 256 bit. which means there are 2^{256} possible AES keys. there is no computer that can perform this search task.

(2) Man-in-the Middle Attack:

Attacker can insert himself between

sender and reciever., who are communicating between them.
before message recieved by reciever it get intercepts before. by attacker

For eg.



Attacker will convince Alice that Attacker is Bob and to Bob that attacker is Alice.
Now. Attacker independently establish connection. with seperate key for both S & R.

(3) Replay Attack:

when attacker replays a valid session between a legitimate user and some form of server.

For eg:

"A" is buying from B's store. and entire transaction is encrypted.
Attacker is able to copy each stage of communication b/w A & B.
After A made purchase. Now Attacker start another session with B. & B will think that A purchasing again.

③ Side - Channel Attacks

these are use unintended side effects of cryptographic operation to glean. information about the plaintext or secret key.

these electric power is used to for encryption - decryption

④ Power Analysis Attack

these computer needs power to run. Amount of power used & how long it have to depend upon operation perform.

Example : for simple Power Analysis (SPA). of RSA algo uses secret key as exponent simple way is to perform sq-&-mult. algo

⑤ Timing Attack :

It expoilt the fact that algo may take different amount of time to run with different plain text

Example : checking of password during login to a secure system.

Question (4)

$$300x + 222y = 6.$$

for coffficient of Bezouts identify (x. and y)

we have

$$300x + 222y = \gcd(300, 222)$$

Applying extended Euclid Algo.

$r_1 = 300$ $\quad$ $r_2 = 222$

$s_1 = 1$ $\quad$ $s_2 = 0$

$t_1 = 0$ $\quad$ $t_2 = 1$

Applying formulae.

$q_1 = r_1 / r_2$, $r = r_1 - q \times r_2$, $r_1 \leftarrow r_2$, $r_2 \leftarrow r$

$s \leftarrow s_1 - q \times s_2$, $s_1 \leftarrow s_2$, $s_2 \leftarrow s$

$t \leftarrow t_1 - q \times t_2$, $t_1 \leftarrow t_2$, $t_2 \leftarrow t$

So,

r_1	r_2	q	r	s_1	s_2	t_1	t_2
300	222	1	78	1	0	0	1
222	78	2	66.	0	1	1	-1
78	66	1	12	1	-2	-1	3
66	12	5	6	-2	3	3	-4
12	6	2	6	3	-17	-4	23.

$\boxed{\gcd = 6, \quad x = -17 \quad , y = 23}$

Hence

$$300(-17) + 222(23) = -5100 + 5106$$
$$= 6.$$

$$\boxed{6 = \gcd(300, 222)}$$

Question ⑦

$$\boxed{P(x) = x^3 + x + 1}$$

primitive elements will be ~~sort of~~ primitive polynomial

Element of $GF(8) = \{0, 1, x, x^2, x^3, x^4, x^5, x^6\}$

$$P(x) = x^3 + x + 1 = 0$$

$$\Downarrow$$

$$x^3 = +1 + x$$

$$\boxed{x^3 = 1 + x}$$

$$x^4 = x(x^3) = (x)(x+1) = x^2 + x$$

$$x^5 = (x)(x^4) = x(x^2 + x) = x^3 + x^2$$
$$= x^2 + 1 + x.$$

$$x^6 = x + x^5 = (x)(x^2 + x + 1) = x^3 + x^2 + x$$
$$= x^2 + 1$$

$\alpha^7 = 1$

$GF(8) = \{0, 1, \alpha, \alpha^2, 1+\alpha, \alpha^2+\alpha, \alpha^2+1, \alpha^2+\alpha+1\}$

Multiplication table :

	0	1	α	α^2	$\alpha+1$	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2+1
0	0	0	0	0	0	0	0	0
1	0	1	α	α^2	$\alpha+1$	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2+1
α	0	α	α^2	$\alpha+1$	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2+1	1
α^2	0	α^2	$\alpha+1$	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2+1	1	α
$\alpha+1$	0	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2+1	1	α	α^2
$\alpha^2+\alpha$	0	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2+1	1	α	α^2	$\alpha+1$
$\alpha^2+\alpha+1$	0	$\alpha^2+\alpha+1$	α^2+1	1	α	α^2	$\alpha+1$	$\alpha^2+\alpha$
α^2+1	0	α^2+1	1	α	α^2	$\alpha+1$	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$

Multiplication table GF(8)

	0	1	2	4	3	6	7	5
0	0	0	0	0	0	0	0	0
1	0	1	2	4	3	6	7	5
2	0	2	4	3	6	7	5	1
4	0	4	3	6	7	5	1	2
3	0	3	6	7	5	1	2	4
6	0	6	7	5	1	2	4	3
7	0	7	5	1	2	4	3	6
5	0	5	1	2	4	3	6	7

Quest (3)

Multiplicative inverse of 24140 in Z^*_{40902} using extended euclidian algo.

$n = 40902 \quad b = 24140.$

n	b	q	r	t_1	t_2
40902	24140	1	16762	0	1
24140	16762	1	7378	1	-1
16762	7378	2	2006	-1	2
7378	2006	3	1360	2	-5
2006	1360	1	646	-5	17
1360	646	2	68	17	-22
646	68	9	34	22	61
68	34	2	0	61	-571

gcd (40902, 24140) = 34 ≠ 1

Hence gcd (40902, 24140) ≠ 1 there is no multiplicative inverse in Z^*_{40902}

Question (2)

Applying gcd Euclidean algorithm.

$$252 = 180(1) + 72$$

$$180 = 72(2) + 36$$

$$72 = 36(2) + 0$$

$$\gcd = 36$$

algo gives $252 > 180 > 72 > 36 > 0$.

The common divisors are the divisors of $\gcd(252, 180) = 36$.

since

$$36 = 2^2 \times 3^2$$

hence common devisor are generated by multiply $\{1, 2, 2^2\}$ and $\{1, 3, 3^2\}$

so, multiples are:

$$\{1, 2, 3, 4, 6, 9, 12, 18, 36\}$$

Question: (6)

subgroups of $G = \langle Z_{16}^*, * \rangle$

$Z_{16} = Z/16 \quad Z = \{[0], [1], [2], [3], \ldots [15]\}$

generators are all the residue classes $[r] \bmod 16$ which give $GCD(r, 16) = 1$.

generators.

$[1]$ $[3]$ $[5]$ $[7]$ $[9]$ $[11]$ $[13]$ $[15]$.

each of the whole grp 2-16.

subgroups are

(i) $\langle [2] \rangle = \{[0], [2], [4], [6], [8], [10], [12], [14]\}$

$= \langle [6] \rangle = \langle [10] \rangle = \langle [14] \rangle$.

(ii) $\langle [4] \rangle = \{[0], [4], [8], [2]\} = \langle [12] \rangle$

(iii) $\langle [8] \rangle = \{[0], [8]\}$, apart from $\{[0]\}$ and 2-16.

Question (5)

Groups of 253 = 52

Possible order of elemen

1, 2, 4, 13, 26, 52

we know $2p^x$ is cycli if p is prim

for each m|52 there are

one $\phi(m)$ eleme order

(i) for each m|52 there is multiplicative subgroup 2^{53} of order m

(ii) for every element order divide the numbe elents of group