1. What do you mean by "Avalanche effect"?

→

The avalanche effect in cryptography refers to the phenomenon where a small change in the input of a cryptographic function, such as a hash function, results in a significant and seemingly unrelated change in the output. This is desirable in cryptographic functions because it makes it difficult for an attacker to predict the output of the function based on partial knowledge of the input.

2. Define Galois Field?

→

Galois Field also known as finite field is a mathematical concept in abstract algebra. It is a set of numbers that consists of a finite number of elements and has two operations that follows specific rules. The rules for the operations ensure that the Galois Field remains closed.

The elements of Galois field $gf(p^n)$ is defined as

$$gf(p^n) = (0, 1, 2, \ldots, p-1) \cup (p, p+1, p+2, \ldots, p+p-1) \cup (p^2, p^2+1, p^2+2, \ldots, p^2+p-1) \cup \ldots \cup (p^{n-1}, p^{n-1}+1, p^{n-1}+2, \ldots, p^{n-1}+p-1)$$

The order of the field is given by p^n while p is called the characteristic of the field. The degree of the polynomial of each element is atmost $n-1$.

3. What is chosen - Ciphertext Attack?

→ In the chosen - ciphertext attack, a cryptanalyst can analyse any chosen ciphertexts together with their corresponding plaintext. The attackers goal is to acquire a secret key or to get as many information about the system as possiable.

The attacker has capability to make the victim decrypt any ciphertext and send him back the result. By analysing the chosen ciphertext and the corresponding received plaintext the intruder tries to guess the secret key which has been used by the victim. Chosen - ciphertext attacks are usually used for breaking systems with public key encryption.

Example :

Suppose A is sending a message to B using a Vigenere Cipher with an unknown key. The enemy is somehow able to intercept the message and replace it with some completely random letters of his own choice, say NLLCJOVFXXHMLY. B decrypts this message and gets AKRUWNBXKWNEYX which is nonsense. Confused and not thinking this nonsense is worth keeping secret, he picks up a non-secure phone and calls A and asks what do you mean by AKRUWNBXKWNEYX. But the enemy is eavesdropping on the line and now knows that NLLCJOVFXXHMLY decrypts to AKRUWNBXKWNEYX. He can then subtract the two sets of nonsense to get MATHMATHMATHMA and now he knows the key

4. What is man-in-the-middle attack?

→

If an attacker puts himself between a client and a webpage, a man-in-the middle attack occures. Man-in-the-middle attack pose a serious threat to online security because they give the attacker the abitily to capture and manipulate sensitive personal information

The Diffie-Hellman key exchange protocol is insecure against a man-in-the-middle attack. Suppose Alice and Bob wish to exchange keys, and Eve is the adversary. In this protocol Eve does not have to find the value of x and y to attack the protocol. Eve can fool Alice and Bob by creating two keys.

The attack proceeds as follows,

i) Eve prepares for the attack by generating two random private keys and then computing the corresponding public keys

ii) Alice chooses x, calculate $R_1 = g^x \bmod p$ and sends R_1 to Bob.

iii) Eve intercepts R_1. choose z and calculate $R_2 = g^z \bmod p$ and sends R_2 to both Alice and Bob.

iv) Bob chooses y, calculate $R_3 = g^y \bmod p$ and sends R_3 to Alice. R_3 is intercepted by Eve and never reaches Alice

v) Alice and Eve calculate $K_1 = g^{xz} \bmod p$ which becomes a shared key between Alice and Eve.

vi) Eve and Bob calculate $K_2 = g^{zy} \bmod p$ which becomes a shared key between Eve and Bob.

5. Find the value of $\phi(32)$, where ϕ denotes Euler's totient function.

→

We have $\phi(32)$

$32 = 8 \times 4 = 2 \times 2 \times 2 \times 2 \times 2$

The prime factor of 32 is 2.

Thus,

$$\phi(32) = 32 * \left(1 - \frac{1}{2}\right)$$

$$= 32 * \frac{1}{2}$$

$$= 16.$$

$\therefore \phi(32) = 16$ Ans

6. Find the value of $\phi(231)$, where ϕ denotes Euler's totient function?

→

We have $\phi(231)$

$231 = 3 \times 7 \times 11$

The prime factors of 231 is 3, 7 and 11

Thus,

$$\phi(231) = 231 * \left(1 - \frac{1}{3}\right) * \left(1 - \frac{1}{7}\right) * \left(1 - \frac{1}{11}\right)$$

$$= \cancel{231} \times \frac{2}{\cancel{3}} \times \frac{6}{\cancel{7}} \times \frac{10}{\cancel{11}}$$

$$= 2 \times 6 \times 10$$

$$= 120$$

$\therefore \phi(231) = 120$ Ans

7. "Meet-in-the-middle" attack is a specific attack for 2-DES - Explain?

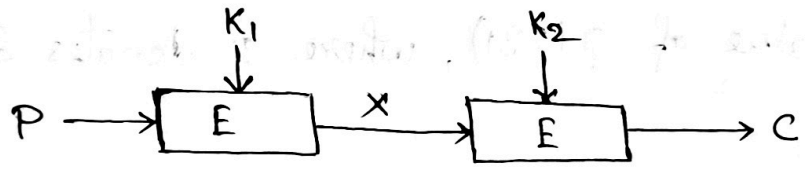
→

The use of double DES results in a mapping that is not equivalent to a single DES encryption. But there is a way to attack this scheme, the algorithm is known as a meet-in-the middle attack. It is on the observation that if we have,

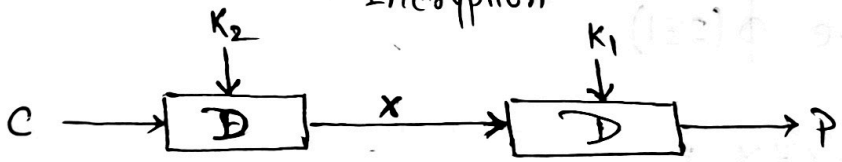
$$C = E(K_2, E(K_1, P))$$

then,

$$X = E(K_1, P) = D(K_2, C),$$



Encryption



Decryption

$$P = D(K_1, D(K_2, C))$$

Given a pair (P, C) the attack proceeds as follows, First encrypt P for all 2^{56} possiable values of the key (K_1). Since these results in a table and then sort the table by the value of X. Next decrypt C using all 2^{56} possiable values of key (K_2). As each decryption is produced check the result against the table for a match. If a match occures

-then test the two resulting keys against a new known plain-text - ciphertext pair. If the two keys produce the correct ciphertext, accept them as the correct key.

For any given plaintext P, there are 2^{64} possible ciphertext values that could be produced by double DES. Double DES uses, in effect a 112 bit key so that there are 2^{112} possible keys. Therefore the foregoing procedure will produce $2^{112}/2^{64} = 2^{48}$ false alarms on the first (P, C) pair. A similar argument indicates that with an additional 64 bit of known plaintext - ciphertext the false alarm rate is reduced to $2^{48}/2^{64} = 2^{-16}$. If a meet-in the middle attack is performed on two blocks of known plaintext - ciphertext the probability that the correct key is determined is $1 - 2^{-16}$.

The result is that the known plain-text attack will succeed against double DES which has a key size of 112 bits with an effort on the order of 2^{56} which is not much more than 2^{55} required for single DES.