PAGE NO.
DATE / /

Tutorial-6

U20CS005

1. Calculate Cipher text C1 & C2 for plain text 7 using Elgamal cryptosystem. Consider public key (2, 8, 11) private key = 3 & r = 4.

→ p = 11, g = 2, e = 8

d = 3, r = 4.

$Y_1 = g^r \bmod p = 2^4 \bmod 11 = 16 \bmod 11$.

$\Rightarrow C_1 = 5$

$Y_2 = M * e^r \bmod p = 7 \times 8^4 \bmod 11$

$= 7 \times 8 \bmod 11 = 28 \bmod 11$

$\Rightarrow C_2 = 6$

∴ Cipher text is (5, 6)//.

2. Explain the process involved in message digest generation & processing of single blak in SHA-1.

→ The process of message digest generation in SHA-1 involves the following steps:

- Padding: The input data is padded so that its length is a multiple of 512 bits. The padding is done by add 1-bit followed by 0-bits and the length of input data in bits in a 64-bit representation.
- Then the padded input is divided into 512 bit blocks & each block is further divided into 16 32-bit words.
- Then the hash value for SHA-1 are initialized to a set of constant.
- Each block of 512 bits is processed using a compression function that operates on a set of five 32-bit intermediate hash values & the 80 word message schedule.
- After processing all blocks through different

rounds & operations, the final hash value is obtained by concatenating the five ~~as~~ obtained hash values in register, and converting them to a fixed length message digest of 160 bits.

5. ~~Given~~ Explain MAC based hash functions with its design objectives & structure of the algorithm.

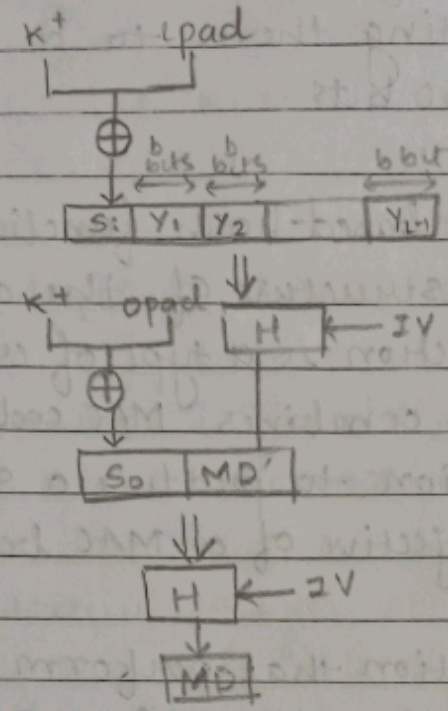
→ - MAC based hash function is a type of cryptographic hash function that combines MAC code with a one-way hash function to produce a secure message digest. The design objective of a MAC based hash function includes:

- To use hash function that perform well on software and for which code is freely and widely available.
- To allow for easy replaceability of the embedded hash function in case faster or ~~some~~ more secure hash function are found or required.
- To preserve original performance of hash function without incurring a significant degradation
- To use & handle keys in a simple way.
- To have a well understood cryptographic analysis of the strength of the authentication mechanism based on reasonable assumption about embedded hash functions.

- Structure of HMAC algorithm:

The working of HMAC starts with taking a message M containing blocks of length b bits. An input signature is padded to the left of the message & whole is given as input to a hash function which gives us a temporary message-digest MD'. MD' again is appended to an output signature and whole is applied ~~to~~ a hash

hash function again, the result is final message digest MD.



Here,
- H stands for hashing fn
- M: original message
- Si & So: I/p & O/p signatures
- Yi - ith block in original message M, where i ∈ [1, L].
- L: count of blocks in M
- K: secret key used for hashing
- IV: initial vector.

$S_i = K^+ \oplus ipad$

$S_o = K^+ \oplus opad$.

$MD' = H(S_i || M)$

$MD = H(S_o || MD')$ or $MD = H(S_o || H(S_i || M))$.

where, K^+ - K padded with zeros on left so that the result is b bits in length

ipad & opad are 00110110 & 01011100 respectively taken b/8 times repeatedly.

4. Given are two protocols in which the sender's party perform the following operation:

- Protocol A: $y = EK1(x || H(K2 || x))$

where x is message, H is hash fn such as SHA-1, E is symmetric key encryption algorithm, E is a public key encryption, "||" denotes concatenation & K1, K2 are secret keys which are only known to sender & receiver.

- Protocol B: $y = x, EKpub(H(x))$

where K is shared secret key, & Kpr is a private key of sender & Kpub is public key of receiver

a) Provide step-by-step description of what the receiver does upon reception of y.

b) State whether the following security services:

- Confidentiality
- Integrity.
- Non-repudiation

is given for each of two protocols given. You have to justify your answer

→ a) Upon reception of y, the receiver does following:

- In case of Protocol A:

- Decrypts y using symmetric key K1 to obtain the concatinated message & hash value $(x \| H(K2 \| x))$.
- Verifies the integrity of message by recomputing the hash value of message using same hash f^n H & second secret key K2 & comparing it with received hash value
- If hash values matches then the message is considered authentic & can be processed further If hash values do not match then the message is considered tampered & must be rejected.

- In case of Protocol B:

- Decrypt the hash value of message using shared secret key k & sender's public key K_{pub} to obtain original hash value
- Computes hash value of message using the same hash f^n H & compares it with received hash value, if it matches the message is considered authentic else it must be rejected.

b).

b) In case of Protocol A:

- Confidentiality: Yes, confidentiality is achieved through encryption.
- Integrity: Yes, it is achieved through hashing.
- Non-repudiation: No, it is not achieved as both parties can claim that other party has created the message. Sender can deny having sent message by claiming that his/her secret key K1 has been compromised & someone else must have used it to encrypt the message.

— In case of protocol B:

- Confidentiality: It is not provided because the message is transmitted in plain text & can be intercepted & read by an attacker.
- Integrity: It is not provide because any-body can replace the message and compute the hash.
- Non-repudiation: It is not provided because sender's private key Kpr is not used to sign message & sender can deny having sent the message.