Page :
Date : / /

Tutorial 6

Q1 Calculate ciphertext C1 & C2 for plaintext = using Elgamal cryptosystem. Consider public key = (2, 8, 11), private key = 3 & r = 4

$p = 11$ $\quad d = 3$
$g = 2$ $\quad r = 4$
$e = 8$

$y_1 = g^r \bmod p$
$= 2^4 \bmod 11$
$= 16 \bmod 11$

$C_1 = 5$

$y_2 = M \times e^{-r} \bmod p$
$= 7 \times 8^4 \bmod 11$
$= 28 \bmod 11$
$C_2 = 6$

$\therefore C = (5, 6)$

Q2 Explain the process involved in message digest generation & processing of single block in SHA-1.

→ 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 & 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 initialised to a set of constant.

→ Each block of 512 bits is processed using a compression function that operates on a set of 5 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 obtained hash values in register and converting them to a fixed length message digest of 160 bits.

Q3 Explain MAC based hash function with its design objectives & structures 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 in software & for which code is freely & widely available.

→ To allow for easy replaceability of the embedded hash function in case faster or more secure hash function are found are found or required.

⇒ 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 funct

25/04/23