Jai Swaminarayan

Ajinkya Rathod (30)

Sem-5

Date / /

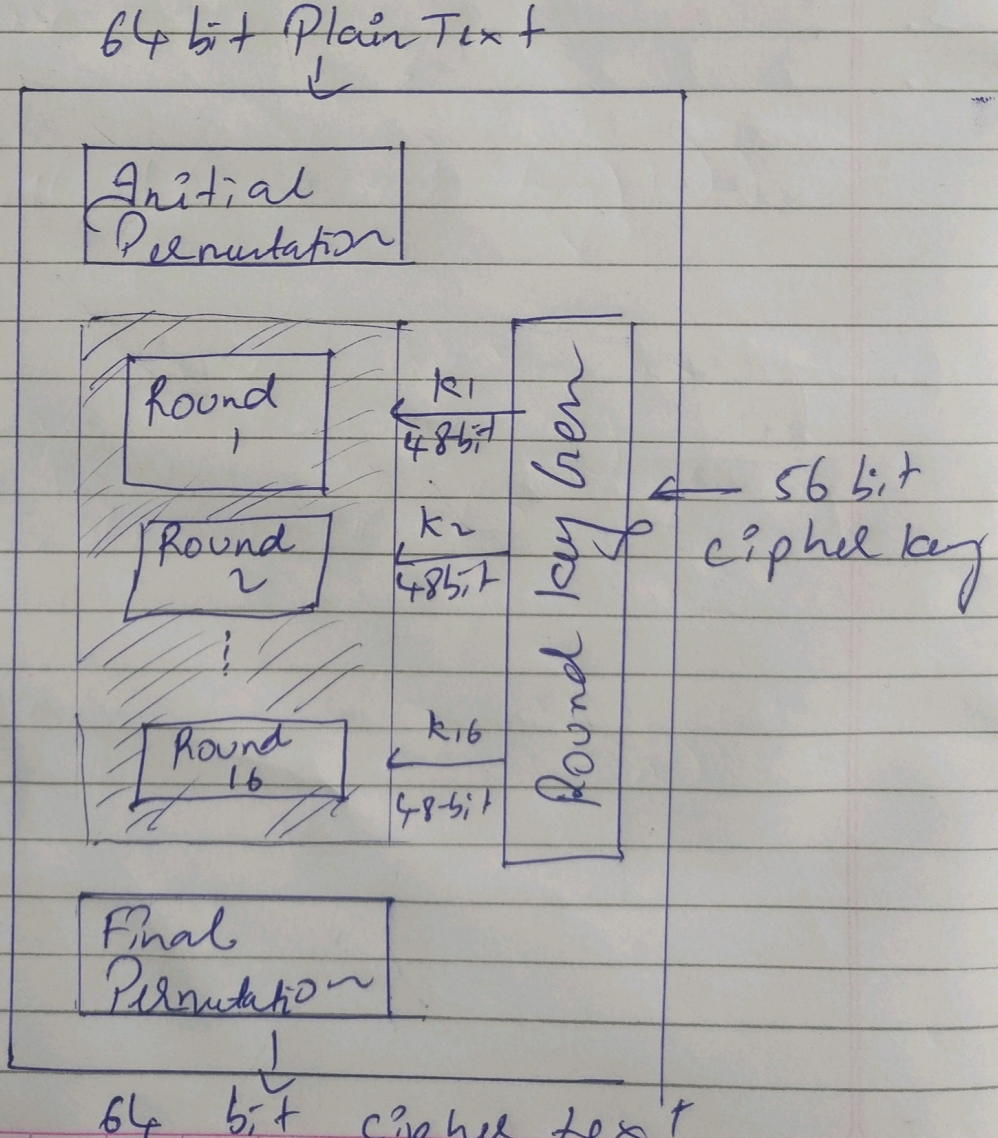
Page 1

Network Security

Q4 DES Algorithm

Ans. The Data Encryption Standard (DES) is a symmetric key block cipher published by the National Institute of Standards and Technology (NIST)

→ It used 16 round Fiestel structure. The Block size is 64-bit.



Since it is based on Feistel Cipher, all that is required to specify DES is:-

- Initial and Final Permutation

→ They are straight and are inverse to each other.

→ They have no cryptography significance in DES.

- Round Function

→ The heart of cipher is DES function. Function f.

→ This DES function applies a 48-bit key to rightmost 32 bits to produce a 32-bit output.

- Key Generation

The round-key generator creates sixteen 48-bit keys out of 56-bit cipher key.

- The logic of Parity Drop, shifting and Compression P-box is implemented

* Analysis

Both DES satisfies properties given below

→ Avalanche Effect

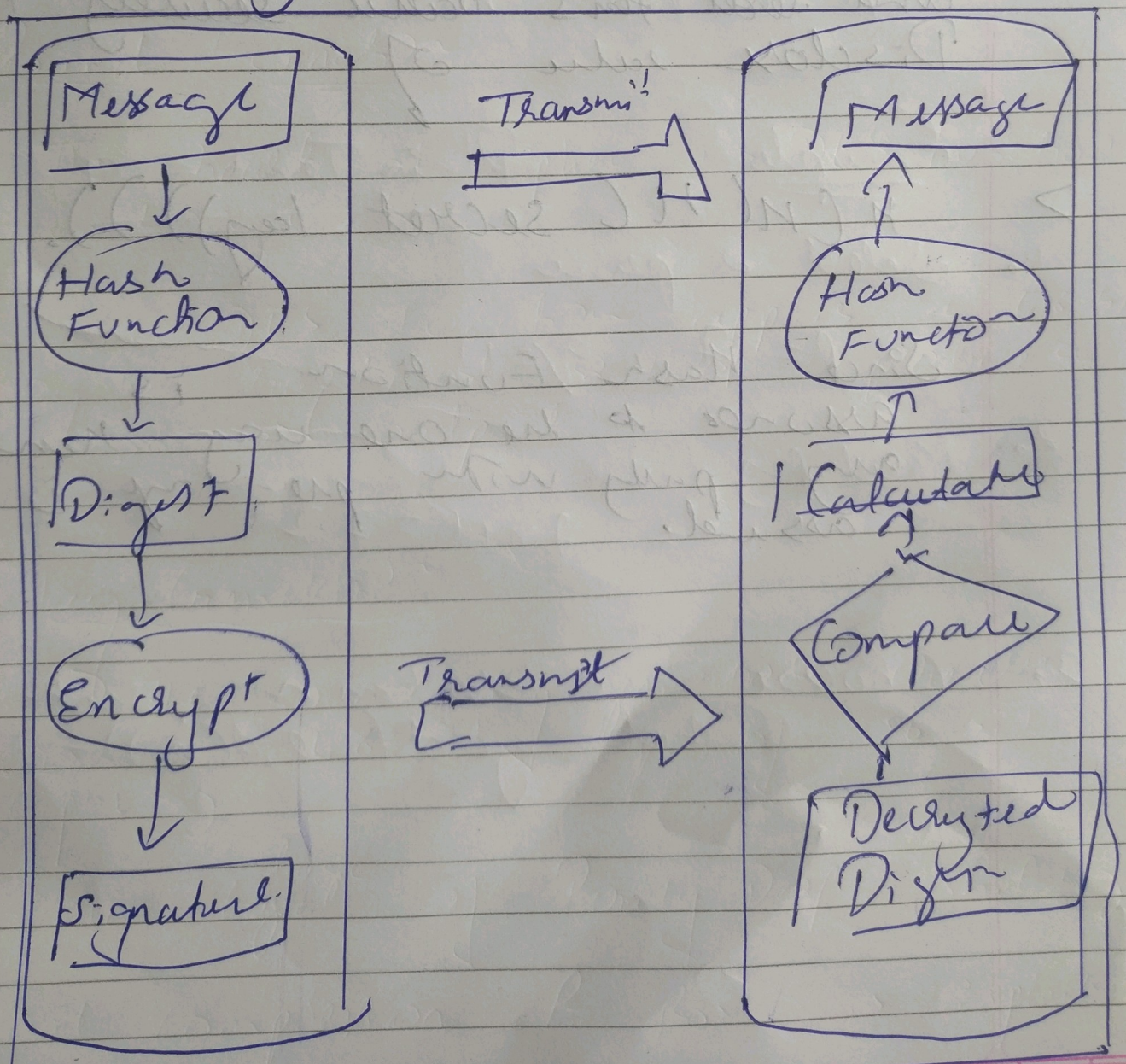
→ Completeness

Date / /
Page 4

Q3 Digital Signature

If one wants to a document with a private signature, anyone can decrypt it but only with a matching public key.

Provided we have kept our key secret and could be a strong evidence.



The basic idea of this chain is to hash a secret key value repeatedly and use of nn hashes or keys in reverse order for authentication.

A simple example would be

> H(H(H(H(secret key))))

and send this value securely to Bob. Disclose value of

> H(H(H(secret key))).

Since Hash Function is assumed to be one way then any party with pre-key is assumed.

Date / /
Page 6

Q2 Steps of RSA

- Select 2 large prime p and q.
- Multiply these numbers to find $n = p \times q$. while n is called moduls for encryption and decryption
- Choose a number e lass than n, such that n is relatively prime to $(p-1) \times (q-1)$. It means that e and $(p-1) \times (q-1)$ have no common factor.

  i.e. $gcd(e, \phi(n)) = 1$.

- If $n = p \times q$ then key is $\langle e, n \rangle$. Plaintext message m is encrypted using public key $\langle e, n \rangle$.
- To find ciphertext from plain, this formula is used.

  $C = m^e \bmod n$.

  (m must be less than n).

- To determine private key, we have formula

$$De \bmod \{(p-1) \times (q-1)\} = 1$$

- Ciphertext "C" is decrypted using private key $\langle d, n \rangle$.

To calculate plain text m :-

$$m = C^d \bmod n$$

Example Plain Text = 9

1. Select 2 prime

$p = 7 \quad q = 11$

2. Multiply

$= 7 \times 11 = 77$

3. Choose e less than n such that $gcd(e, \phi(n)) = 1$.

$$\phi(n) = (p-1) \times (q-1)$$

$$\phi(n) = (7-1) \times (11-1)$$

$$= 6 \times 10$$

$$= 60$$

Choosing relative prime as 7.

Thus key is (7, 77)

4. $C = m^e \bmod n$

$9^7 \bmod 77$

$C = 37$

5. $De \bmod \{(p-1) \times (q-1)\} = 1$

$7d \bmod 60 = 1$

$(\because d = 43)$

So, $\langle d, n \rangle = (43, 77)$

6. $m = C^d \bmod n$

$= 37^{43} \bmod 77$

$\underline{\underline{m = 9}}$ (∴ So we got initial plaintext)

Thus the plaintext = 9

ciphertext = 37

Q5 In Brief

a. Integrity

→ It is fundamental required of trustworthy identity infrastructure.

→ Identity systems exchange credentials as well as messages and transactions regarding attributes, provisioning information and other data.

→ In this, we have that trusting that the contents have not been tampered with is important

b. Non-Repudiation

Non-Repudiation is a presentation of unforgeable evidence that a ~~text~~ message was sent or received.

→ If messages or transaction can be disputed, then important of identity action can

me jeopaldized.

C. Product Cipher

→ It combines two or more transformation in manner intending that the resulting cipher is more secure than the individual components to make it resistant to cryptanalysis.

→ It combines a sequence of simple transformation such as

⇒ (1) S-Box (Substitution Box)

(2) P- Box (Permutation Box)

(3) Modular Arithmetic

Q. Confidentiality

Ans The most common ways of confidentiality are

-> Steganography
-> Encryption

a. Steganography is a the process of putting a message inside another message in such a way that observer never know it is there

b. Encryption is process of transforming a message using a key that anyone viewing the message without key cannot determine its contents.

MD5, DES, RSA are common examples of encryption

2. Asymmetric key Cryptography

- It is a cryptographic system that uses a pair of keys.
- Each pair consists of a public key and a private key.
- The generation of such key pair depends on algos which are based on maths.
- In such systems, any person can encrypt a message using intended recievers public key.

But that encrypted msg can only be decoded with recievers private key.