Register Number | | | | | | | | | |

Sri Sivasubramaniya Nadar College of Engineering, Kalavakkam – 603 110

(An Autonomous Institution, Affiliated to Anna University, Chennai)

Department of Computer Science and Engineering

Continuous Assessment Test– III

Question Paper

Degree & Branch	B.E CSE				**Semester**	V
Subject Code & Name	UCS1505 - INTRODUCTION TO CRYPTOGRAPHIC TECHNIQUES				**Regulation: 2018**	
Academic Year	2020-21	**Batch**	2018-22	**Date**	**2.11.20**	**FN**
Time: 90 Minutes	**Answer All Questions**				**Maximum: 50 Marks**	

Part – B Answer any TWO questions (2×10 = 20 Marks)

<KL3>	1 a. Represent in a diagrammatic form the tasks in public key encryption scheme that happen between sender and receiver. Modify the above diagram, to show the adversary forgery in public encryption scheme. (3) b. Define one-way function. List few examples of one-way function. (4) c. What is meant by pseudo random generator, pseudo random function, and pseudo random permutation. (3)	<CO5> / <CO4>
<KL3>	2 a. Why we need hybrid encryption? Explain Hybrid encryption using the KEM/DEM paradigm (4) b. What are the applications of public key crypto systems? Define RSA digital signature. Find the signature for p=823, q=953, e=313, d=160009, m=19070. (6)	<CO5>

INTRODUCTION TO CRYPTOGRAPHIC TECHNIQUES

CAT-3.

Date : 2/11/20

SHASHANKA VENKATESH
185001145 CSE-"C"

Part-B

2. Ans:

We need hybrid encryption due to the following facts about Public-key encryption:

Fact 1: CPA security & Eavesdropping security are equivalent ⇒ the attacker doesn't gain anything from being able to query the encryption oracle

Fact 2: Any deterministic encryption scheme is not CPA-secure.

Fact 3: Plain RSA is not CPA-secure

Fact 4: NO Public key Crypto system can achieve Perfect secrecy //

To overcome all these shortcomings of pure public key encryption, Hybrid Encryption was introduced.

Private key encryptions are also more efficient than public key ones.

Hybrid Encryption can be done using the key Encapsulation Mechanism:

The key-encapsulation mechanism (KEM) is a triple of ppt algorithms (Gen, Encaps, Decaps) such that:

1) Gen on input 1^n outputs a pair of keys (pk, sk). Both have length at least n & n can be determined from pk

2) Encaps on input pk and 1^n outputs a ciphertext c and a key $k \in \{0,1\}^{l(n)}$, where l is the key length.

$$(c, k) \leftarrow Encaps_{pk}(1^n)$$

3) Decaps is deterministic and takes as input sk & c and outputs a key k or $\perp$.

$$k := Decaps_{sk}(c)$$

So, using KEM:

1) Sender runs $Encaps'_{pk}(1^n)$ to obtain c & k

2) Then uses some private key encryption scheme to encrypt m (actual message) using k yielding c'

3) He sends c & c'

Now,

4) The reciever uses c to compute k (private key used) as $k := Deccaps_{sk}(c)$ [using his private key]

5) Then, he decrypts the actual message using the key obtained ⇒ $m := Dec'_k(c')$

b. Ans:

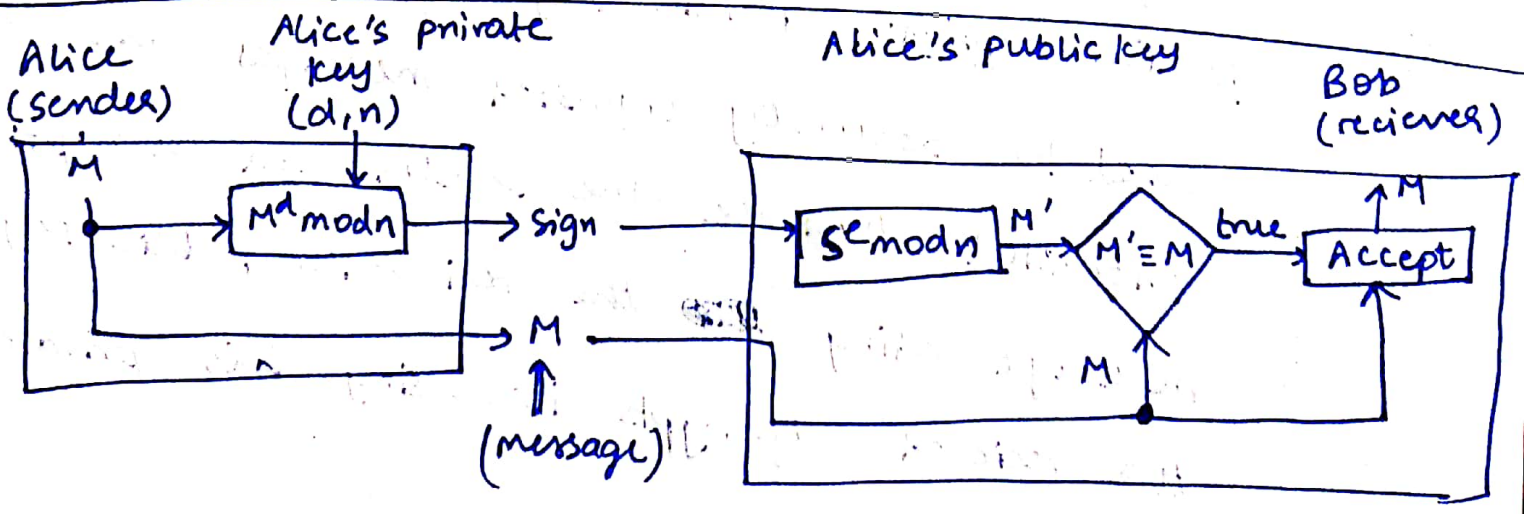
Applications of public key crypto systems:

1) Encryption: Public key crypto systems can be used to securely transfer messages over an untrusted channels. The sender can encrypt the message using the reciever's public key and the reciever decrypts it using his private key.

2) Digital Signature: This is a very frequently used application of public key crypto systems. It can be used to authenticate the message sent by someone, whose public key is known. The sender encrypts the message using his private key and sends it. The reciever can verify the message by decrypting the signature sent. The sender might hash the message before encrypting it, since otherwise, the signature will become too long. The reciever hashes the message before verification in that case //.

RSA Digital Signature:

In the RSA digital signature scheme, d is private; e & n are public:



Basically, the sender encrypts the message (or the hash of the message) using his private key, (d, n). He then sends both the Message & the encrupted message (which is a signature) The reciever takes the signature & decrypts it using the Sender's public key and verifies that the decrypted signature & message are the same.

$p = 823$

$q = 953$

$e = 313$

$d = 160009$

$m = 19070$

Find signature:

In RSA digital signature,

$$S = (m^d) \bmod n$$

now, $n = p \times q = 823 \times 953 = \boxed{784319}$

$\Rightarrow S = (19070^{160009}) \bmod 784319$

$S = \boxed{210625}$ $\Rightarrow$ this is the signature sent along with the message //

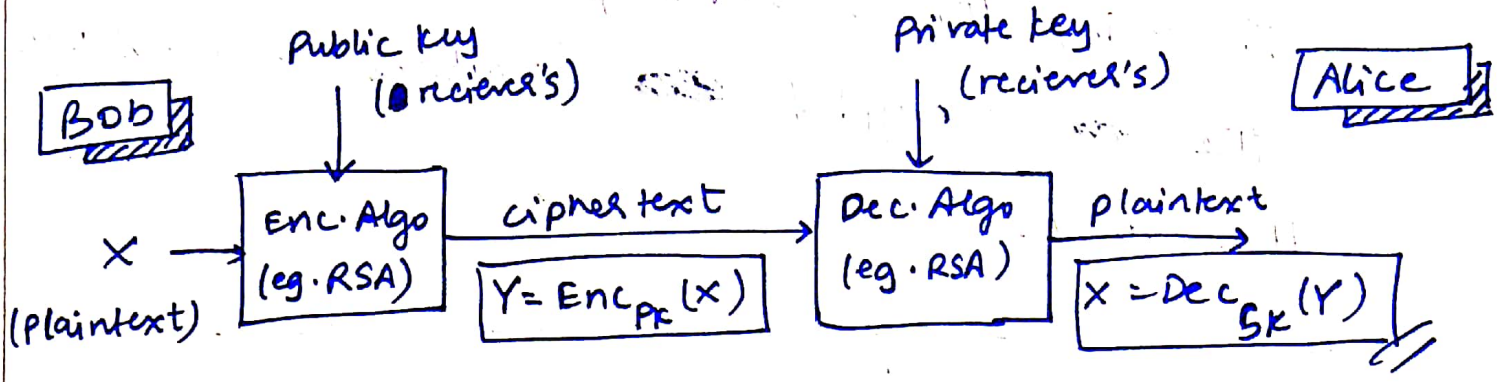
1. Ans:

a) Public key Encryption:

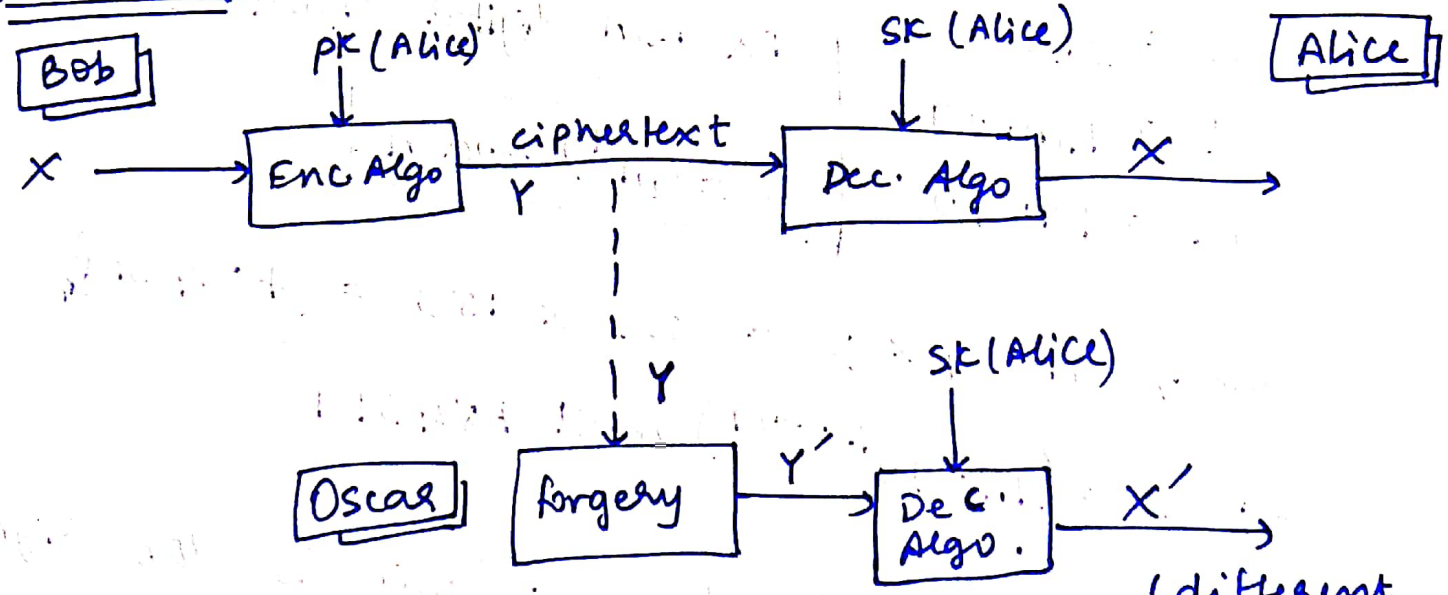
1) Sender encrypts using reciever's public key

2) Reciever decrypts using his/her private key.

Diagramatic rep:



Adversary: (Oscar):



In this way, the adversary can send forged messages

b) One-way function:

A one-way function is a function that maps a domain of values onto a range, such that every function value has a unique inverse, with the condition that the calculation of the function is easy, whereas the inversion is infeasable:

$Y = f(x)$ is easy → polynomial time

$X = f^{-1}(Y)$ is infeasable → exponential time

then, f is a one-way function.

Basically, probability of finding the inverse should be such that there is a function $negl(x)$ such that:

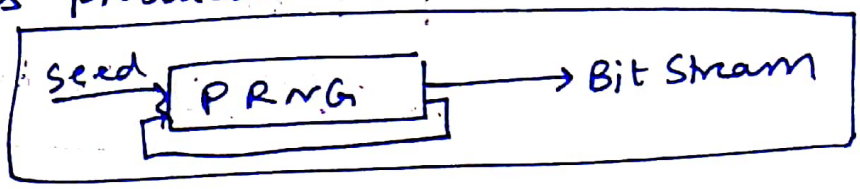
$$Pr[Inverse_A, f(x) = 1] \leq negl(x)$$

Examples: SHA-1, SHA-256, Discrete Logarithm etc. (they should be collission resistant or have a pseudorandom permutation)

//

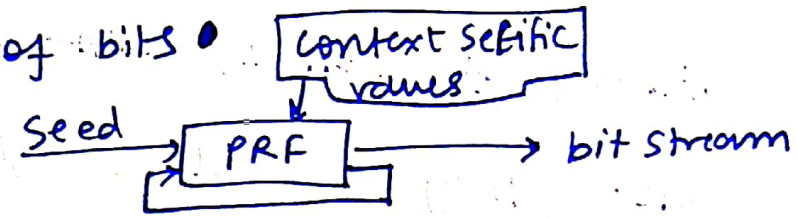
c) Pseudo-random generator.

A pseudo random generator (PRNG) is an algorithm that is used to produce an open-ended sequence of bits. It requires a seed (from a truly random source), since this is a deterministic algorithm. The PRNG uses the truly random seed to produce a pseudo random number. It always produces the same value for the same seed.



Pseudo-random function:

A pseudo-random function (PRF) is used to produce a pseudorandom string of bits of fixed length. It takes a seed as input & some context specific values. The main (and only) difference between PRNG & PRF is the no. of bits.



Pseudo-random permutation (PRP)

A pseudo-random permutation has 3 elements:

$K, X, X \Rightarrow$ $E : K \times X \rightarrow X$

A PRP is bijective and has an efficient (polynomial time) inverse. Even they are deterministic.

PRP's are sometimes called block ciphers //

Part C

1) Ans:

i) Diffie Hellman key Exchange:

DHKE is a public key crypto system using discrete logarithm //

A & B use DHKE using common prime $q = 11$ & primitive root $\alpha = 2$

A & B exchange a key. A selects $x_A < q$ & computes $Y_A = \alpha^{x_A} \bmod q$

B selects $x_B < q$ & computs $Y_B = \alpha^{x_B} \bmod q$

x_A & x_B are private

Y_A & Y_B are publicly sent.

A recieves Y_B & computes $K: (Y_B)^{X_A} \bmod q$

B recieves Y_A & computes $K: (Y_A)^{X_B} \bmod q$ //

a) $q = 11 \quad \alpha = 2 \quad Y_A = 9$

$Y_A = \alpha^{X_A} \bmod q$

$\Rightarrow 9 = 2^{X_A} \bmod 11 \Rightarrow \boxed{X = 6}$ //

b) $Y_B = 3 \quad Y_A = 9, \alpha = 2, q = 11$

$\Rightarrow$ Secret key,

$K = (Y_B)^{X_A} \bmod q$

$\Rightarrow K = 3^6 \bmod 11$

$= 729 \bmod 11$

$\Rightarrow \boxed{K = 3}$ shared key is 3 //

ii) RSA algorithm:

$p = 11, q = 13, e = 11, M = 7$

Step 1: key generation.

Select p & q [both prime, $p \neq q$]

$\Rightarrow$ Select 11 & 13

Calculate $n = p \times q \Rightarrow n = 11 \times 13 = \boxed{143}$

Select integer e [such that $\gcd(\phi(n), e) = 1$ & $1 < e < \phi(n)$]

Here, $\boxed{e = 11}$

Calculate d [$d = e^{-1} \pmod{\phi(n)}$]

Here, $d = 11^{-1} \bmod 120$

$\boxed{d = 11}$

public key $\Rightarrow$ $PU = \{e, n\} \Rightarrow \boxed{\{11, 143\}}$

private key $\Rightarrow$ $PR = \{d, n\} \Rightarrow \boxed{\{11, 143\}}$

Step 2:

Encryption Plaintext $M < n$

$$C = M^e \bmod n$$

$$\Rightarrow C = 7^{11} \bmod (143)$$

$$\boxed{C = 106}$$

Step3 Decryption:

Ciphertext C

Plaintext. $\boxed{M = C^d \bmod n}$

$$\Rightarrow M = 106^{11} \bmod 143$$

$$\Rightarrow \boxed{M = 7}$$

Original message recieved back