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 – I

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**	**4.9.20**	**FN**
Time: 90 Minutes	**Answer All Questions**				**Maximum: 50 Marks**	

Part – A Answer all the questions (10×2 = 20 Marks)
(MCQ type – Randomly post 10 questions to the student)

<KL3>	1. Let M=C=K={0,1,2,… 255}, and consider the following cipher defined over {K,M,C}: E(k,m)=m+k (mod 256); D(k,m)=c-k (mod 256). Does This have perfect secrecy? a. No. There is a simple attack on this cipher b. No. only the one time pad has perfect secrecy c. **Yes** d. It would, if 255 were a prime number	<CO3>
<KL2>	2. The three concepts that form what is often referred to as the CIA triad are _____ . These three concepts embody the fundamental security objectives for both data and for information and computing services. A) **confidentiality, integrity and availability** B) communication, integrity and authentication C) confidentiality, integrity, access control D) communication, information and authenticity	<CO1>
<KL2>	3. A loss of _____ is the unauthorized disclosure of information. A) authenticity B) **confidentiality** C) reliability D) integrity	<CO1>
<KL2>	4. Kerchkhoff's Principle preaches to open their design of the encryption algorithm and rely on the diverse range of key values (represented by key length). Why try to keep Crypto algorithm secret will not work? a. By making the algorithm secret, it will encourage hackers to steal it b. **By making it open for commenting / experiments, it allows more experts to work the detection of the weakness, Potential bugs and exploits**.	<CO1>
<KL2>	5. What are the differences between Substitution Cipher and Transposition Cipher? a. The substitution Cipher reorders the letters of the plaintext but do not disguise them. The transposition preserves the order of the symbols of the plaintext while mapping them uniquely to different symbols. b. **The substitution Cipher preserves the order of the symbols of the plaintext while mapping them uniquely to different symbols. The transposition Cipher reorders the letters of the plaintext but not to disguise them**.	<CO1>
<KL2>	6. Restoring the plaintext from the ciphertext is _____ . A) **deciphering** B) transposition C) steganography D) encryption	<CO1>

<KL2>	7. A _____ attack involves trying every possible key until an intelligible translation of the ciphertext is obtained. A) **brute-force** B) Caesar attack C) ciphertext only D) chosen plaintext	<CO1>
<KL2>	8. How many keys are required for two people to communicate via symmetric and asymmetric ciphers? a. **1, 2** b. 2,1 c. 2,2 d 1, Many	<CO1>
<KL2>	9. What are the general approaches to attacking a cipher? a. **Cryptanalysis and brute force** b. Brute force c. Intrusion d. Steganography	<CO1>
<KL3>	10. what is the probability of getting the sum 4 while throwing 2 dies. a. **3/36** b. 1/6 c. 4/36 d. 6/36	<CO3>
<KL3>	11. What is the probability of Pr[M = 'hi' | C = 'xy'] given that ; Pr[M='hi'] = 0.3, Pr[M='no'] = 0.2, Pr[M='in']= 0.5 Using Shift cipher **a. 0.6** b. 0.3 c. 0.2 d. 0.5	<CO3>
<KL3>	12. What is the key used to decrypt the cipher text XS HIGVCTX E QIWWEKI, using shift cipher a**. 4** b. 15 c. 23 d. 24	<CO3>
<KL3>	13. Use Caesar's Cipher to decrypt the following QHWZRUNLQJ SRVVLELOLWLHV a.. ENCRYPTION MALLEABILITY b. **NETWORKING POSSIBILITIES** c. TECHNOLOGY PROGRESSING d. NETWORKING MALLEABILITY	<CO3>
<KL3>	14. If "thisiscryptography" is encrypted using Vigenère cipher system, with the key as "FIND", the cipher text is a. **ypvvnapudxgrlznsmg** b. ypvvxypuddgrlznsmg c. ypvvnapudxgrhtnvxy d. Ypvvxypuddingznsmy	<CO3>
<KL3>	15. The following word was encrypted using a Caesar cipher with a shift of 2: ecguct. What word is it? * a. romans b. cipher c. julius d. **Caesar**	<CO3>
<KL2>	16. Caesar Cipher is an example of * a. Poly-alphabetic Cipher b. **Mono-alphabetic Cipher** c. Multi-alphabetic Cipher d. Bi-alphabetic Cipher	<CO1>
<KL2>	17. Monoalphabetic ciphers are stronger than Polyalphabetic ciphers because frequency analysis is tougher on the former. *	<CO1>

	a. True b. **False**	
<KL3>	18. Consider the shift cipher for all k: {1, ..., 25}. Pr[M = 'i'] = 0.6, Pr[M = 'c'] = 0.4. What is Pr[C = 't']? a. 0.3855 b. **0.04** c. 0.06 d. 0.0385	<CO3>
<KL3>	19, Consider the shift cipher for all k: {0, ..., 25}, and the distribution Pr[M= 'bvn'] = 0.25, Pr[M= 'ict'] = 0.75. What is Pr[C = 'eyp']? a. 0.038 b. **0.029** c. 0.009 d. 0.042	<CO3>
<KL3>	20. Consider one-time pad over message space of 4 bit strings. Pr[M=1000] = 0.2 and Pr[M=0111] = 0.8. What is Pr[C=0000]? a. 0.016 b. 0.025 c. **0.0625** d. 0.0125	<CO3>

Part – B Answer all the questions (2×5 = 10 Marks)

<KL2>	1 Provide a formal definition of the Gen, Enc, and Dec algorithms for the mono-alphabetic substitution cipher.	<CO1>
<KL3>	2 Caesar wants to arrange a secret meeting with Marc Antony, either at the Tiber (the river) or at the Coliseum (the arena) . He sends the shift cipher text EVIRE. However, Antony does not know the key, so he tries all possibilities. Where will he meet Caesar?	<CO3>

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

<KL3>	3 Prove that the cryptosystem built using the above probability is perfectly secure? P(X=a) =1/2, P(X=b) =1/3, P(X=c) =1/6, P(K=k1) =P(K=k2) =P(K=k3) =1/3	<CO3>
<KL3>	4a. Prove that if only a single character is encrypted, then the shift cipher is perfectly secret. (5) (b) What is the largest message space M for which the mono-alphabetic substitution cipher provides perfect secrecy? (5)	<CO3>
<KL2>	5a. Define pseudorandom Generator and its properties (5) b.Write a brief note about private key encryption? (5)	<CO1>

Prepared By	Reviewed By	Approved By
Course Coordinator	PAC Team	HOD

SSN COLLEGE OF ENGINEERING
RECORD SHEET

Sheet No.....

CAT-1

UCS1505 - Introduction to Cryptographic techniques

Name: B. VIGNESH

Sem & Sec: 5 'C'

Reg no : 185001193

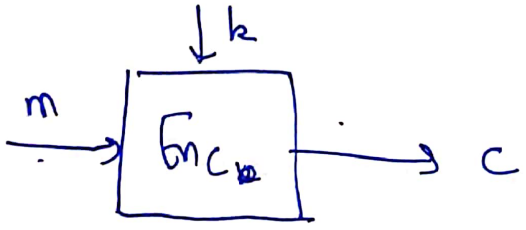
Date : 4/9/20

1) A private key encryption scheme is defined by a message M and algorithms (Gen, Enc, Dec):

① The key generation algorithm Gen is a probabilistic algorithm that outputs a key k chosen according to some distribution.
It outputs $k \in K$

② The encryption algorithm Enc takes as input a key k and a message m and outputs a ciphertext c. We denote by $Enc_k(m)$ the encryption of the plaintext m using the key k.

$$c \leftarrow Enc_k(m)$$



Dec (decryption algo) : The decryption algo Dec takes as input a key k and a ciphertext c and outputs a plaintext m. We denote the decryption of the cipher text c using the key k by $Dec_k(c)$

$$m \leftarrow Dec_k(c)$$

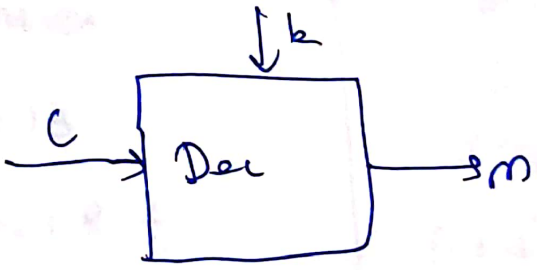
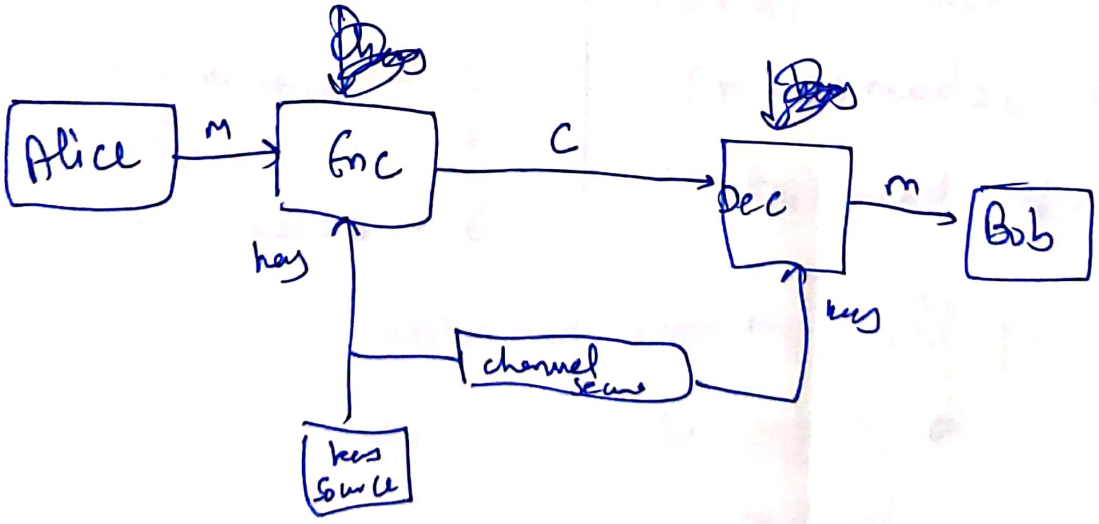


Fig Decryption.



Usage in Private key encryption

Mono alphabetic ciphers:

① It is implemented with permutation technique of 26 alphabetical letters.

② A letter can be mapped on a one to one relationship with any letter.

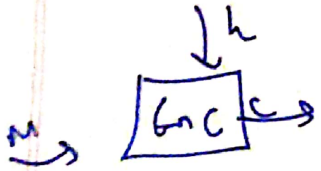
③ Gen algorithm: (key gen algorithm):

In this algorithm, the key to encrypt is generated i.e. gives an output 'k' according to the set methodology.

here $k = 0, 1, 2 \ldots 25$ for each number is $\in k$

④ Encryption algo:

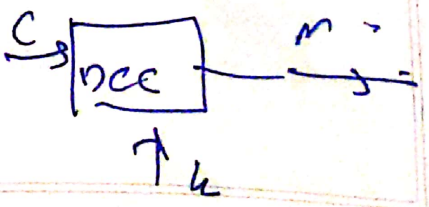
It takes input from 'k' and a message m and output is a ciphertext c.



$$C_\pi(m) = \pi(m)$$

⑤ Decryption: takes input k and ciphertext c and output is plain text

$$D_\pi(c) = \pi(c)$$



(2)

Let M_1 = river

M_2 = arena

C = EVIRE

Case 1 :-

m = river

shift = 13

C = EVIRE

(r + 13) mode 26 = E

(i + 13) mod 26 = V

(v + 13) mod 26 = I

(e + 13) mod 26 = R

(r + 13) mod 26 = E

Case 2 :-

m = arena

C = EVIRE

shift = 4

(a + 4) mod 26 = E

(r + 4) mod 26 = V

(e + 4) mod 26 = I

(n + 4) mod 26 = R

(a + 4) mod 26 = E

Since the key is unknown, even trying all possibilities of the key, dec(EVIRE) can be arena or river using key = 4 and key = 13 respectively.

∴ The probability of both = 50%.

Antony cannot determine the where he may meet Cleo or if he cannot even know where he goes for

Part-C

3) Checking for perfectly secure system:

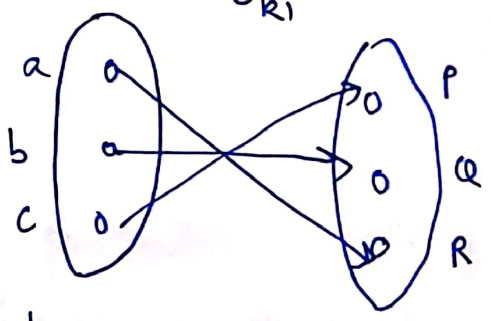
$P(X=a) = 1/2$

$P(X=b) = 1/3$

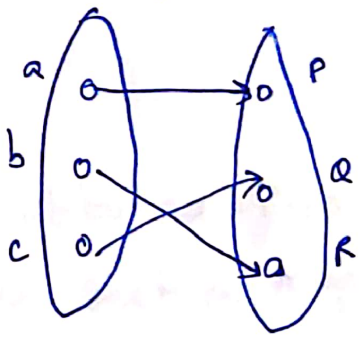
$P(X=c) = 1/6$

$P(K=k1) = P(K=k2) = P(K=k3) = 1/3$

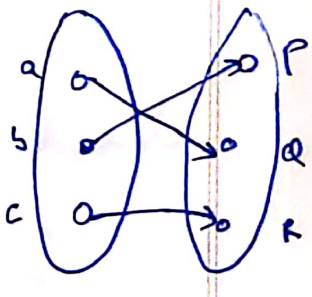
e_{k1}



e_{k2}



ek_3



Ciphertext probabilities:

$$Pr[Y=y] = \sum_k Pr(k).Pr(d_k(y))$$

$$Pr[Y=P] = Pr(k_1).Pr(c) + Pr(k_2).Pr(a) + Pr(k_3).Pr(b)$$

$$= \frac{1}{3} * \frac{1}{6} + \frac{1}{3} * \frac{1}{2} + \frac{1}{3} * \frac{1}{3} = \frac{1}{3}$$

$$Pr[y = Q] = Pr(k_1).Pr(b) + Pr(k_2).Pr(c) + Pr(k_3)\,Pr(a)$$

$$= \frac{1}{3} * \frac{1}{3} + \frac{1}{3} * \frac{1}{6} + \frac{1}{3} * \frac{1}{2} = \frac{1}{9} + \frac{1}{18} + \frac{1}{6}$$

$$= \frac{1}{3}$$

$$Pr[y = R] = Pr(k_1)\,Pr(a) + Pr(k_2).Pr(b) + Pr(k_3).Pr(c)$$

$$= \frac{1}{3} * \frac{1}{2} + \frac{1}{3} * \frac{1}{3} + \frac{1}{3} * \frac{1}{6} = \frac{1}{6} + \frac{1}{9} + \frac{1}{18}$$

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

The probability that y is obtained given x depends on the keys which provide such a mapping

$$Pr[y|x] = \sum_{\{k: d_k(y) = x\}} Pr[k]$$

$$Pr(P|a) = Pr(k_2) = \frac{1}{3}$$

$$Pr(Q|a) = Pr(k_3) = \frac{1}{3}$$

$$Pr(R|a) = Pr(k_1) = \frac{1}{3}$$

$P(P|b) = Pr(k_3) = \frac{1}{3}$

$P(Q|b) = Pr(k_1) = \frac{1}{3}$

$P(R|b) = Pr(k_2) = \frac{1}{3}$

$P(P|c) = Pr(k_1) = \frac{1}{3}$

$P(Q|c) = Pr(k_2) = \frac{1}{3}$

$P(R|c) = Pr(k_3) = \frac{1}{3}$

Computing posteriori Probability:

$$Pr[x|y] = \frac{Pr[x] \times Pr[y|x]}{Pr[y]}$$

x = plaintext
y = ciphertext.

$$Pr[a|P] = Pr[a] * \frac{Pr[P|a]}{Pr[P]} = \frac{1}{2} * \frac{\frac{1}{3}}{\frac{1}{3}} = \frac{1}{2}$$

$$Pr[a|Q] = Pr[a] * \frac{Pr[Q|a]}{Pr[Q]} = \frac{1}{2} * \frac{\frac{1}{3}}{\frac{1}{3}} = \frac{1}{2}$$

$$Pr[a|R] = Pr[a] * \frac{Pr[R|a]}{Pr[R]} = \frac{1}{2} * \frac{\frac{1}{3}}{\frac{1}{3}} = \frac{1}{2}$$

$$Pr[b|P] = Pr[b] * \frac{Pr[P|b]}{Pr[P]} = \frac{1}{3} * \frac{\frac{1}{3}}{\frac{1}{3}} = \frac{1}{3}$$

$$Pr[b|Q] = Pr[b] * \frac{Pr[Q|b]}{Pr[Q]} = \frac{1}{3} * \frac{\frac{1}{3}}{\frac{1}{3}} = \frac{1}{3}$$

$$Pr[b|R] = Pr[b] * \frac{Pr[R|b]}{Pr[R]} = \frac{1}{3} * \frac{\frac{1}{3}}{\frac{1}{3}} = \frac{1}{3}$$

From above,

$$Pr[a|P] = Pr[a|Q] = Pr[a|R] = Pr[X=a]$$

$$Pr[b|P] = Pr[b|Q] = Pr[b|R] = Pr[X=b]$$

Since $Pr[x|y] = Pr[x]$

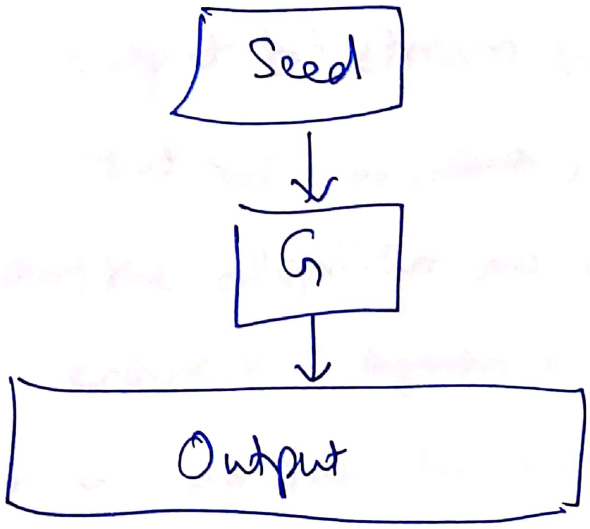
i.e. attacker learns nothing from cipher text.

Since posteriori probability = a priori probabilities.

∴ The system is perfectly secret.

5) a) A PRG is an efficient, deterministic algorithm that expands a short, uniform seed into a larger, pseudorandom output.

Let G be a deterministic poly-time algorithm that is expanding, i.e. $|G(x)| = P(|x|) > |x|$



G defines a sequence of distributions.

TRNG (True random no generator): Takes as input a source that is random.

The source is referred to as entropy source.
Eg keystroke, clock.

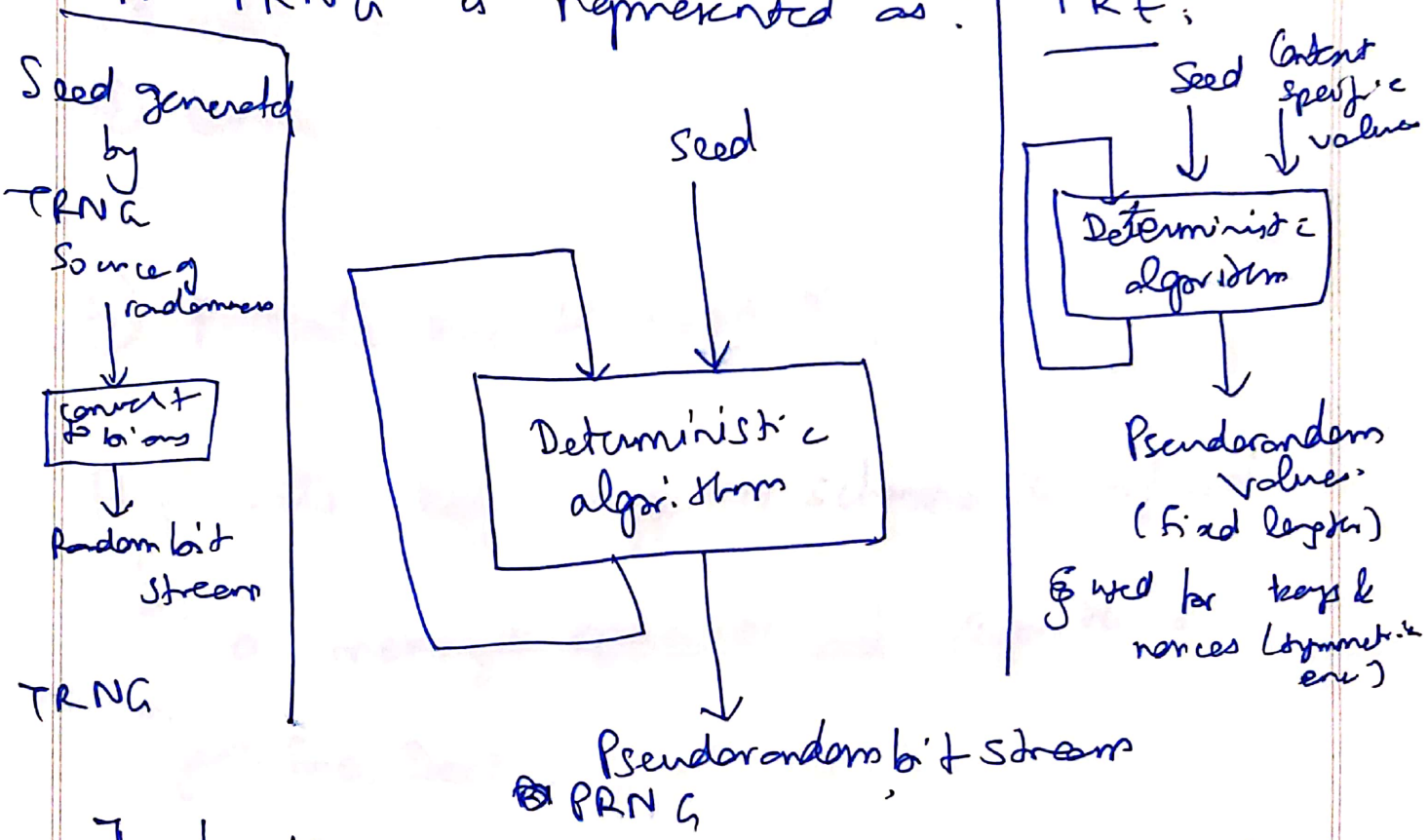
It involves converting analog source to binary output.

Pseudorandom Number Generator & its properties:

- It takes as input a fixed value, called the seed, and produces a sequence of output bits using a deterministic algorithm.
- The seed used is generated by using a true random number generator (TRNG)
- The output bit stream is determined solely by the input value or values, so an adversary who knows the algorithm and the seed can reproduce the entire bit ~~system~~ stream.
- It is similar to Pseudorandom functions only difference being in no. of bits produced.
- It is an algorithm that is used to produce an open-ended sequence of bits.

- It is used as input to a symmetric stream cipher.

A PRNG is represented as:



The basic requirement when a PRNG is used for cryptographic applications is that an adversary who does not know the seed is unable to determine the pseudorandom string.

The specific requirement are as follows:

- Randomness
- Unpredictability
- Characteristics of the seed.

The random number so produced must pass three characteristics:

1. Uniformity
2. Scalability
3. Consistency

b) Private key encryption:

A private key encryption scheme is defined by a message space M and algorithms (Gen, Enc, Dec):

- Gen (key generation algorithm): outputs $k \in K$
- Enc: The key generation algorithm Gen is a probabilistic algorithm that outputs a key k chosen according to some distribution.

* Enc (encryption algorithm) : takes key k and message $m \in M$ as input outputs cipher text c

$$c \leftarrow Enc_k(m)$$

The Enc algorithm is denoted by $Enc_k(m)$ the encryption of plain text m using the key k.

* Dec (decryption algorithm) : takes key k and cipher text c as input ; outputs m or "error"

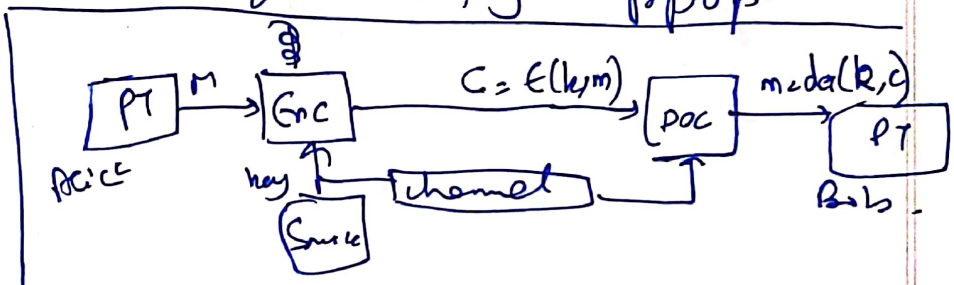
For all $m \in M$ and k output

$$Dec_k(Enc_k(m)) = m$$

The decryption of the cipher text c using the key k is denoted by $Dec_k(c)$.

Contd...

Private key encryption is the form of encryption where only a single private key can encrypt & decrypt the info. It is a fast process as it uses single key. However protecting and key creates management issue. The key may be stolen or leaked hence requiring changing of algorithm and distributing appropriate keys.



key

k

ciphertext

(c)

key k.

Alice
m

Bob

$C = Enc_k(m)$

$m = Dec_k(c)$

m = plaintext
c = ciphertext

Private key encryption.