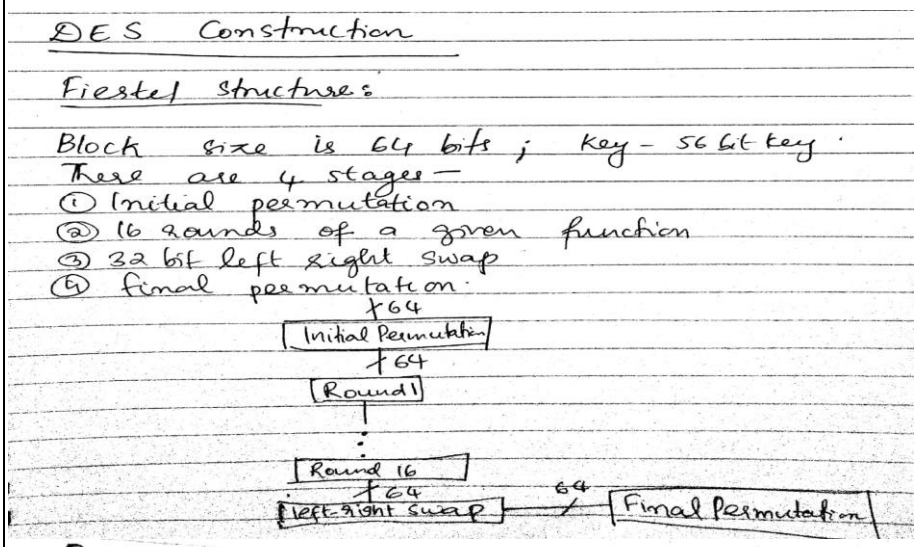
USN | | | | | | | | | | |

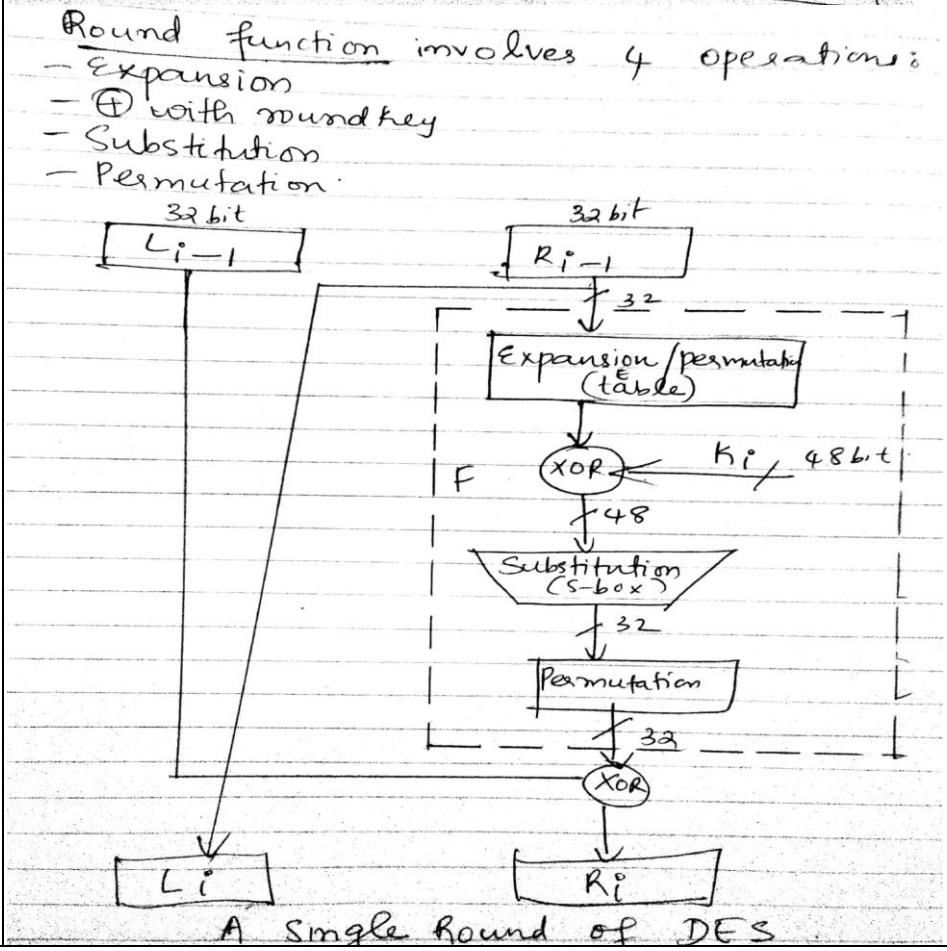
Internal Assessment Test 1 – March 2018

Sub:	Cryptography, Network Security and Cyber Law					Sub Code:	15CS561	Branch:	CSE	
Date:	12/03/2018	Duration:	90 min's	Max Marks:	50	Sem / Sec:	VI/A,B,C		OBE	

Answer any FIVE FULL Questions

		MARKS	CO	RBT
Q1.	Explain DES with neat block diagrams. Diagrams (2+4=6M) Explanation (4M)	[10]	CO1	L2





64-bit plain text passes through an initial permutation that rearranges the bits to produce permuted input. This is followed by a phase consisting of 16 rounds of the same function, which involves both permutation and substitution. The o/p of the last round consists of 64 bits that are a function of input plain text and key. The left and right halves of output are swapped to produce preoutput. the preoutput is passed through inverse permutation to produce 64-bit cipher text.

Details of a single round – The left and right halves of each 64-bit ~~plaintext~~ values are treated as separate 32-bit values (L) and (R). The input to the round function is R_{i-1} which is expanded to 48 bits. 48 bits is then ⊕ed with round key, k_i (derived from main key, different for each round). The result of ⊕ operation is divided into eight 6-bit chunks. (8 S-boxes) ∴ O/p of S-box 4-bit (eight 4-bit chunks which is of total 32 bits). This output is then passed to permutation table. ~~to which~~

For encryption,

$$L_i = R_{i-1}$$

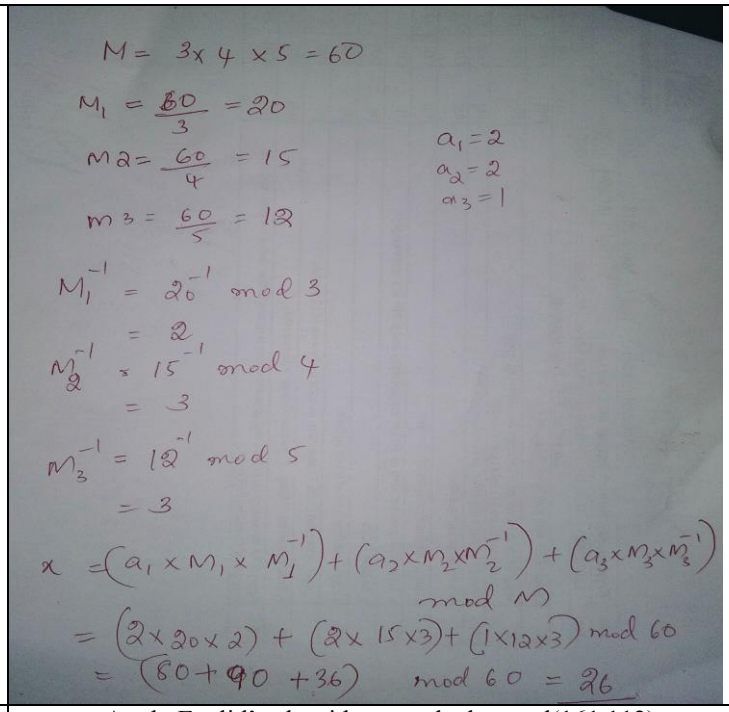
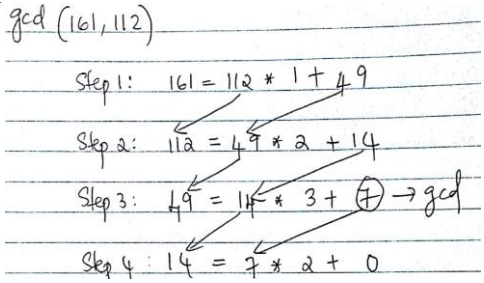
$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

For Decryption,

$$R_{i-1} = L_i$$

$$L_{i-1} = R_i \oplus f(L_i, K_i)$$

Q2.	Apply Chinese Remainder Theorem for following input, $x \cong 2 (\text{mod } 3), x \cong 2 (\text{mod } 4), x \cong 1 (\text{mod } 5)$ M1,M2,M3- (3 M), Inverses (4M), Final calculation (3M)	[10]	CO1	L3

				
Q3.	a. Apply Euclid's algorithm to calculate gcd(161,112). Each step carries 1 Mark. 	[05]	CO1	L3
	b. Explain phishing, DoS. Phishing – (2.5M) DoS-(2.5M) ① Phishing and pharming attacks: These attacks attempt to retrieve personal information from an individual. In phishing attack, the attacker directs its victims to a fake website (eg: banking site) which has the look and feel of authentic site where the victim has to share his credentials (username / password) which are then passed on to the attacker. ④ Denial of Service (DoS) :- These attacks are meant to exhaust the computing power, memory capacity or bandwidth and make the service interrupted. It usually slows down the system.	[05]	CO1	L2
Q4.	Explain Guiding Principles of security.	[10]	CO1	L2

Following are certain principles of modern security practice.

1) Security is as much a human problem than a technological problem and must be addressed at different levels.

At the highest level, security should be addressed by top-level management. In large organizations. Robust security policies should be formulated and implementation strategy must be outlined by a team headed by CISO (Chief Information Security Officer).

System administrators should be proactive in patch application, configuring s/ms & applications, setting user/group permissions to various s/m resources.

The final link in the security chain is the rank & file within an organization. Employees should be educated on do's & don'ts through security awareness programs.

2) Security should be factored in at inception, not as an afterthought.

Functionality, correctness, performance, and reliability hogged the attention of designers several years ago. Integrating secure coding practices into the application software would be a solution to numerous attacks. Security should be enforced in early on during the design phase of a new product & then carried forward right through implementation & testing.

3) Security by obscurity (or by complexity) is often bogus.

The flaws are exposed over time after the protocols have been widely deployed, attracting closer attention from the hacker community. Ethical hackers community should be atleast study new protocols & algorithms prior to widespread adoption.

	④ Always consider the "Default Deny" policy for adoption in access control. The tradeoffs b/w White listing & black-listing should be carefully examined. Prudent security design should seriously consider adoption of the "Default Deny" policy. ⑤ An entity should be given the least amount/level of permissions/privileges to accomplish a given task. - RBAC - Privilege escalation ⑥ Use 'Defence in Depth' to enhance security of an architectural design. - Firewalls. ⑦ Identify vulnerabilities & respond appropriately. Risk = Assets × Vulnerability × Threats ⑧ Carefully study the tradeoffs involving security before making any. - Security vs cost - Security vs performance - Security vs convenience			
Q5.	a. Write difference between secret key cryptography and public key cryptography. SKC –(2.5 M) PKC-(2.5M)	[5]	CO1	L2
	Secret key cryptography - The sender and receiver share a common secret - for encryption & decryption. So $e = d$ in the above equation. If Alice and Bob share a secret key, k then she encrypts the message using the common secret. The encrypted message is decrypted using the same secret. Operation performed by Alice : $c = E_k(p)$ Operation performed by Bob : $p = D_k(c)$ eg: DES, AES. Public key Cryptography — Two distinct keys forming a key pair are used — encryption key or public key and decryption key or private key. Public key of user → to encrypt message to that user. It is known to everyone. Private key → to decrypt message. It should not be revealed to anyone. If Alice and Bob use public key cryptography,			

Alice would encrypt her message using Bob's public key. Then Bob decrypts the message using his private key.
Operation performed by Alice:

$C = E_{B.pu}(P)$, B.pu → public key of Bob

$P = D_{B.pr}(C)$, B.pr → private key of Bob

eg: RSA, ECC.

b. Explain PKCS [5] CO2 L2

The use of small encryption keys is not secure and a solution is to pad the message with non-zero random bits before performing encryption. The number and positions of these bits are standardized. Padding is important if the message contains data that can be guessed. An attacker could guess plaintext, encrypt it with ~~plain text~~ public key and verify whether its encrypted version coincides with ciphertext sent.

PKCS #1, specified the format of data to be encrypted by RSA. Bytes of block from left should be 00 followed by 02 followed by at least 8 random non-zero bytes and other.

00	02	PAD	00	Plain text

Q6. a. Explain different substitution ciphers. [5] CO2 L2

Caesar – 2M, Vigenere- 1.5 M, Hill- 1.5M

① Monoalphabetic ciphers

Substitution technique is one in which the letters of plain text are replaced by other letters or by numbers or symbols. In monoalphabetic cipher, the ciphes text corresponding to a particular character in the plain text is ~~not~~ fixed.

– Caesar Cipher → In this, each alphabet in the text is replaced by the alphabet k positions away. For k=3, substitutions are

D for A, E for B, A for X, ...

Plain text: what is the population of Mars

Cipher text: zkdw lv wkh srsxodwlrq ri Pduv

Encryption, $C = (P+3) \bmod 26$, (k=3)

Decryption, $P = (C-3) \bmod 26$.

② Polyalphabetic Ciphers

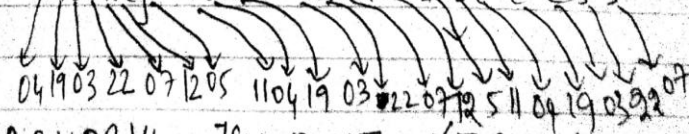
In this, ciphertext corresponding to a particular character in the plaintext is not fixed.

The Vigenere Cipher

It uses multi-digit key, $k_1, k_2, \ldots k_m$
The plain text is split into non-overlapping blocks, each containing m consecutive characters. Then the first letter of each block is replaced by letter k_1 positions to its right, ...

eg: key – 04 19 03 22 07 12 05 11

Plain text: Wishing You Much Success



Hill Cipher

The plain text is broken into blocks of size m. The key in Hill cipher is $m \times m$ matrix of integers between 0 and 25.

We use the mapping $A \to 0, B \to 1, \ldots, Z \to 25$

Let $p_1, p_2, \ldots, p_m$ be the plain text,
$c_1, c_2, \ldots, c_m$ be the ciphertext.

$$c_1 = p_1 k_{11} + p_2 k_{21} + \cdots + p_m k_{m1} \bmod 26$$

$$c_m = p_1 k_{1m} + p_2 k_{2m} + \cdots + p_m k_{mm} \bmod 26$$

$C = PK$ → Encryption
$P = CK^{-1}$ → Decryption.

Decryption will fail if K is singular.

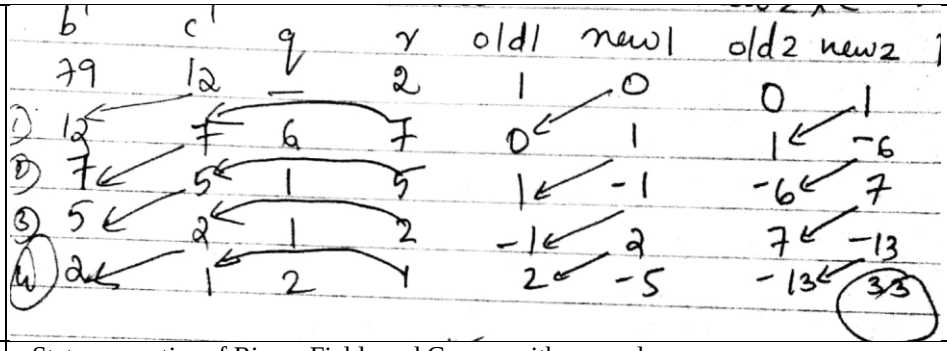
eg: ① P = (H I) $K = \begin{pmatrix} 3 & 7 \\ 15 & 12 \end{pmatrix}$

H → 7, I → 8

Here m = 2.

$$C = PK = (7 \quad 8) * \begin{pmatrix} 3 & 7 \\ 15 & 12 \end{pmatrix} \bmod 26$$

	b. Apply extended Euclid's algorithm to calculate inverse of 12 modulo 79.	[5]	CO2	L3

					
Q7.	a. State properties of Rings ,Fields and Groups with example. Groups(4M) , ring(3M), field (3M)	[10]	CO1	L2

Groups – A group is a pair $\langle G, * \rangle$ where G is a set and * is a binary operation such that following properties hold :

① closure : If $a, b \in G$, $a * b \in G$

② Associativity : If $a, b, c \in G$, then
$a * (b * c) = (a * b) * c$

③ Identity element : There exists I in G such that for all b in G,
$I * b = b = b * I$

④ Inverse : For each element b in G, there exists exactly one element c in G such that
$b * c = c * b = I$.

eg : Set of integers with addition $(Z, +)$ – is a group.
– closed
– Associative
– identity : 0 ; $a + 0 = a$
– inverse : $-a$; $a + -a = 0$

Rings

Ring is a triplet $\langle R, +, * \rangle$ + and * are binary operations and R is a set satisfying

(i) $\langle R, + \rangle$ is a commutative group.

(ii) For all x, y and z in R,

$x * y \in R$

$x * (y * z) = (x * y) * z$ (Associative)

$x * (y + z) = (x * y) + (x * z)$ (Distributive)

Few other properties —

(1) All rings that we use have multiplicative identity = 1.

(2) * need not be commutative, if * is commutative, then it is commutative ring.

(3) Each element x in R has an additive inverse $(-x)$.

eg: $(Z, +, *)$ — Infinite ring

$(Z^+, +, *)$ — not a ring because all set numbers except 0 do not have additive inverse.

Fields

A field $\langle R, +, * \rangle$ is a commutative ring with following properties:—

(1) R has a multiplicative identity = 1

(2) Each element x in R has an x^{-1}. $x x^{-1} = 1$.

eg: $\langle R, + \rangle$ and $\langle R - \{0\}, * \rangle$ are commutative groups.

Set of all real numbers with + and * — Infinite field.

No. of elements in a field is p^m. (p - prime, m - +ve integer)

A field of size p^m: $GF(p^m)$

For m = 1,

$GF(p) = \langle Z_p, +_p, *_p \rangle$.

For m > 1 fields, they are represented as Polynomials of degree m−1 over Z_p.

Q8.	Apply RSA to encrypt 00111011 and generate cipher text, and further derive the plain text with decryption. Consider P=3,q=11. Encryption (5M), Decryption (5M)	[10]	CO2	L3

$n = pq = 11 \cdot 3 = 33$

$\phi(n) = (p-1)(q-1) = 10 \cdot 2 = 20$

choose e, such that $\gcd(e, 20) = 1$

let $e = 3$.

$d = e^{-1} \bmod \phi(n)$

$= 3^{-1} \bmod 20$

$= 7$

$b = \lceil \log_2 33 \rceil = 6$ (divide m to 6 bits each)

I message block = 001110 = 14 (First 6 bits)

Second block = 000011 = 3 (pad first 4 bits with zero)

$c_1 = m_1^e \bmod n$

$= 14^3 \bmod 33 = 5$

$c_2 = m_2^e \bmod n$

$= 3^3 \bmod 33$

$= 27$

Decryption —

$m_1 = c_1^d \bmod n$

$= 5^7 \bmod 33$

$= 14$

$m_2 = c_2^d \bmod n$

$= 27^7 \bmod 33$

$= 3$