Internal Assessment Test 1- Oct. 2024

SCHEME & SOLUTION

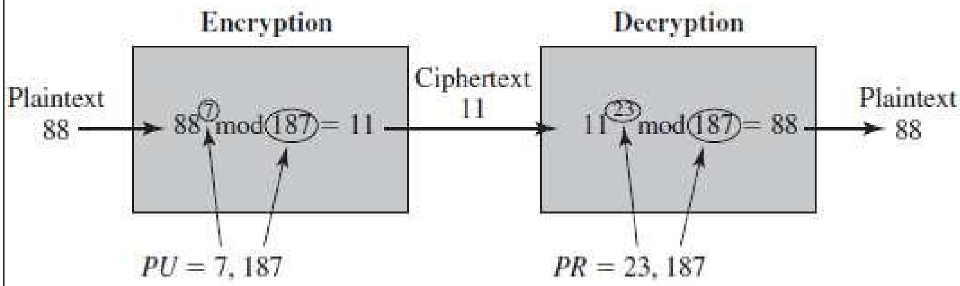
<table>
<tr><td></td><td>Cryptography and Network Security</td><td>Sub Code:</td><td>21IS71</td><td>Branch:</td><td colspan="2">ISE</td></tr>
<tr><td colspan="4"><u>Answer any FIVE FULL questions</u></td><td>MARKS</td><td>CO</td><td>RBT</td></tr>
<tr><td>1</td><td colspan="3">What are crypto systems?. Explain general Caesar algorithm. Construct cipher text for the plain text “ meet me after the toga party ” using Caesar algorithm.

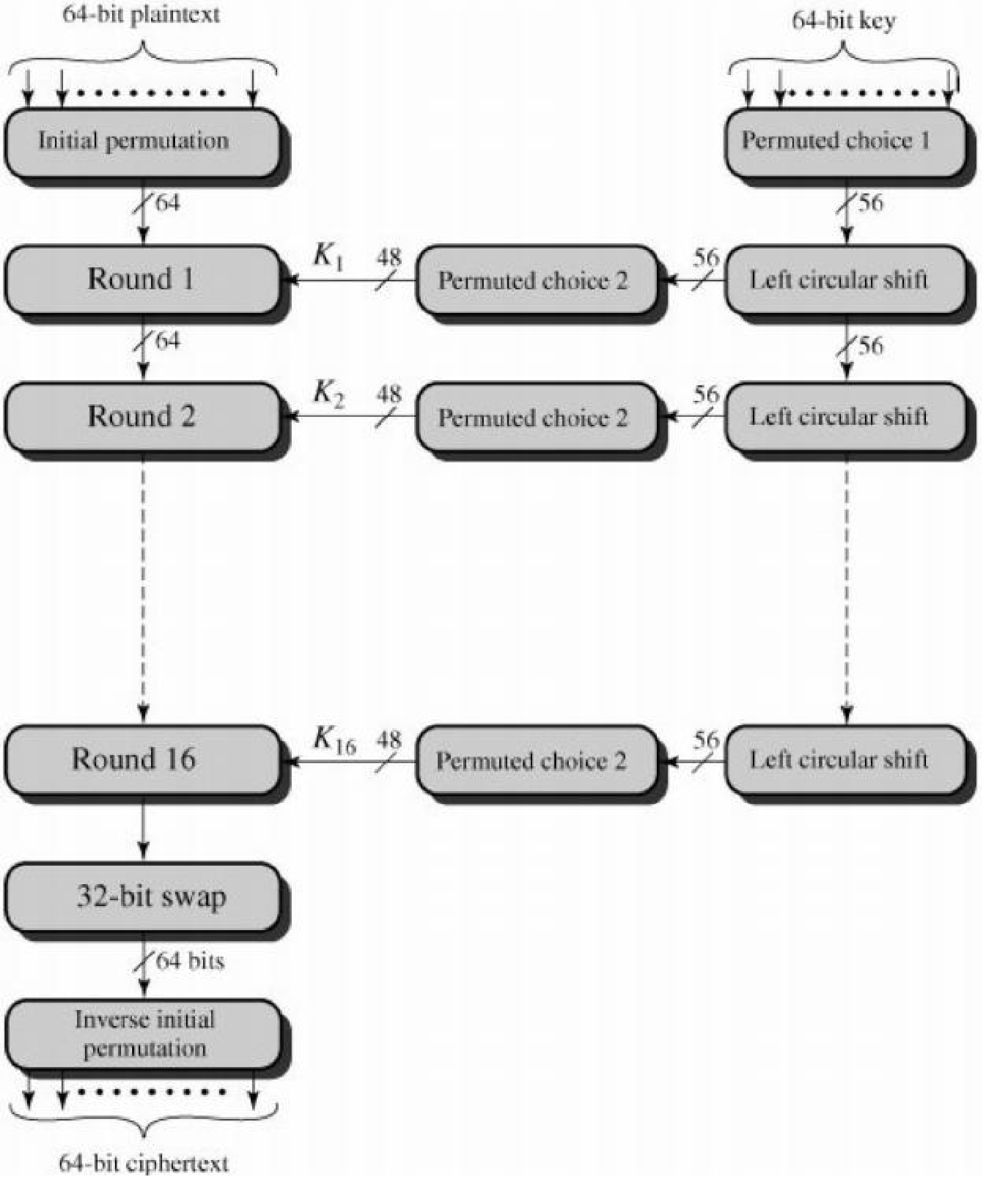
The systems that are capable of encrypting and decrypting data before being stored or transmitted in network are called crypto systems.
Caesar Cipher:
The algorithm can be expressed as follows. For each plaintext letter p, substitute the ciphertext letter C:
$C = \mathrm{E}(3, p) = (p + 3) \bmod 26$
A shift may be of any amount, so that the general Caesar algorithm is
$C = \mathrm{E}(k, p) = (p + k) \bmod 26$
where k takes on a value in the range 1 to 25. The decryption algorithm is simply
$p = \mathrm{D}(k, C) = (C\ k) \bmod 26$
If it is known that a given ciphertext is a Caesar cipher, then a brute-force cryptanalysis is easily
performed: Simply try all the 25 possible keys.

For example,
plain: meet me after the toga party
Cipher: PHHW PH DIWHU WKH WRJD SDUWB</td><td>2+5+3
[10]</td><td>CO1</td><td>L3</td></tr>
<tr><td>2</td><td colspan="3">Using Key word “Monarchy”, explain Playfair Cipher generation method.

The best-known multiple-letter encryption cipher is the Playfair, which treats digrams in the plaintext as single units and translates these units into ciphertext digrams.
The Playfair algorithm is based on the use of a 5 x 5 matrix of letters constructed using a keyword. Here is an example,
M O N A R
C H Y B D
E F G I/J K
L P Q S T
U V W X Z
In this case, the keyword is monarchy. The matrix is constructed by filling in the letters of the keyword (minus duplicates) from left to right and from top to bottom, and then filling in the remainder of the matrix with the remaining letters in alphabetic order.
The letters I and J count as one letter. Plaintext is encrypted two letters at a time, according to the following rules:
1. Repeating plaintext letters that are in the same pair are separated with a filler letter, such as x, so that balloon would be treated as ba lx lo on.
2. Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last. For example, ar is encrypted as RM.
3. Two plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the column circularly following the last. For example,</td><td>4+6 [10]</td><td>CO1</td><td>L3</td></tr>
</table>

	mu is encrypted as CM. **4.** Otherwise, each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter. Thus, hs becomes BP and ea becomes IM (or JM, as the encipherer wishes).			
3	Apply Hill cipher encryption and decryption on the following message. Text Message: "paymoremoney" Use the encryption key: $\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$ a. Show your calculations for encryption and decryption b. Construct cipher text **HILL CIPHER:** The first three letters of the plaintext are represented by the vector $\begin{pmatrix} 15 \\ 0 \\ 24 \end{pmatrix}$. Then $\mathbf{K}\begin{pmatrix} 15 \\ 0 \\ 24 \end{pmatrix} = \begin{pmatrix} 375 \\ 819 \\ 486 \end{pmatrix} \bmod 26 = \begin{pmatrix} 11 \\ 13 \\ 18 \end{pmatrix}$ = LNS. Continuing in this fashion, the ciphertext for the entire plaintext is LNSHDLEWMTRW. Decryption requires using the inverse of the matrix **K**. The inverse **K-**1 of a matrix **K** is defined by the equation **KK-**1 = **K-**1**K** = **I.** In this case, the inverse $\mathbf{K}^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$ This is demonstrated as follows: $\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}\begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} = \begin{pmatrix} 443 & 442 & 442 \\ 858 & 495 & 780 \\ 494 & 52 & 365 \end{pmatrix} \bmod 26 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ It is easily seen that if the matrix **K-**1 is applied to the ciphertext, then the plaintext is recovered. In general terms, the Hill system can be expressed as follows: **C** = E(**K, P**) = **KP** mod 26 **P** = D(**K, P**) = 1**C** mod 26 = 1 **KP** = **P**	[10]	CO1	L3
4	Using RSA Algorithm show encryption and decryption of plaintext message M=88. Assume p=17,q=11 and e=7. **Example:** **1.** Select two prime numbers, $p = 17$ and $q = 11$. **2.** Calculate $n = pq = 17 \times 11 = 187$. **3.** Calculate $\varnothing(n) = (p - 1)(q - 1) = 16 \times 10 = 160$. **4.** Select e such that e is relatively prime to $\varnothing(n) = 160$ and less than $\varnothing(n)$; we choose $e = 7$. **5.** Determine d such that $de \equiv 1 \pmod{160}$ and $d < 160$. The correct value is $d = 23$, because 23 * 7 = 161 = (1 × 160) + 1; The resulting keys are **public key *PU* = {7, 187}** and **private key *PR* = {23, 187}.**	5+5 [10]	CO2	L3

	 Figure 9.6 Example of RSA Algorithm **For encryption,** Calculate $C = 88^7 \bmod 187$. Exploiting the properties of modular arithmetic, we can do this as follows. $88^7 \bmod 187 = [(88^4 \bmod 187) \times (88^2 \bmod 187) \times (88^1 \bmod 187)] \bmod 187$ $88^1 \bmod 187 = 88$ $88^2 \bmod 187 = 7744 \bmod 187 = 77$ $88^4 \bmod 187 = 59{,}969{,}536 \bmod 187 = 132$ $88^7 \bmod 187 = (88 \times 77 \times 132) \bmod 187 = 894{,}432 \bmod 187 = 11$ **For decryption,** Calculate $M = 11^{23} \bmod 187$. $11^{23} \bmod 187 = [(11^1 \bmod 187) \times (11^2 \bmod 187) \times (11^4 \bmod 187) \times (11^8 \bmod 187) \times (11^8 \bmod 187)] \bmod 187$ $11^1 \bmod 187 = 11$ $11^2 \bmod 187 = 121$ $11^4 \bmod 187 = 14{,}641 \bmod 187 = 55$ $11^8 \bmod 187 = 214{,}358{,}881 \bmod 187 = 33$ $11^{23} \bmod 187 = (11 \times 121 \times 55 \times 33 \times 33) \bmod 187 = 79{,}720{,}245 \bmod 187 = 88$			
5	Using Feistel Cipher structure explain DES Algorithm As with DES encryption scheme the plaintext must be 64 bits in length and the key is 56 bits in length. Looking at the left-hand side of the figure, we can see that the processing of the plaintext proceeds in three phases. First, the 64-bit plaintext passes through an initial permutation (IP) that rearranges the bits to produce the *permuted input*. This is followed by a phase consisting of 16 rounds of the same function, which involves both permutation and substitution functions. The output of the last (sixteenth) round consists of 64 bits that are a function of the input plaintext and the key. The left and right halves of the output are swapped to produce the **preoutput**.	6=4 [10]	CO1	L2

<table>
<tr><td></td><td>

Finally, the preoutput is passed through a permutation (IP-1) that is the inverse of the initial permutation function, to produce the 64-bit ciphertext. With the exception of the initial and final permutations, DES has the exact structure of a Feistel cipher, as shown in Figure.</td><td></td><td></td><td></td></tr>
<tr><td>6</td><td>a) Explain Public Key Cryptosystems.

Public key cryptography for providing confidentiality (secrecy)

There is some source A that produces a message in plaintext X = [X1, X2, . . . ,XM].
The M elements of X are letters in some finite alphabet. The message is intended for destination B.
B generates a related pair of keys: a public key, PUb, and a private key, PRb.
PRb is known only to B, whereas PUb is publicly available and therefore accessible by A.</td><td>2+2+2
[06]</td><td>CO2</td><td>L2</td></tr>
</table>

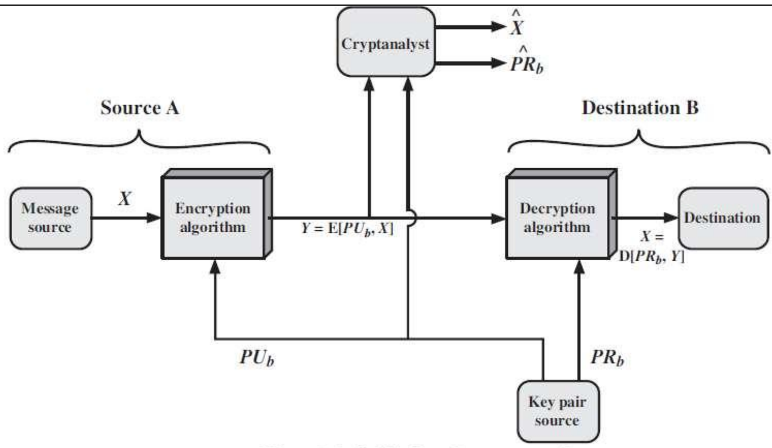


Figure 9.2 Public-Key Cryptosystem: Secrecy

With the message X and the encryption key ***PUb*** as input, A forms the ciphertext $Y = [Y1, Y2, \ldots, YN]$: $Y = E(PU_b, X)$

The intended receiver, in possession of the matching private key, is able to invert the transformation:

$$X = D(PR_b, Y)$$

Public key cryptography for proving Authentication:

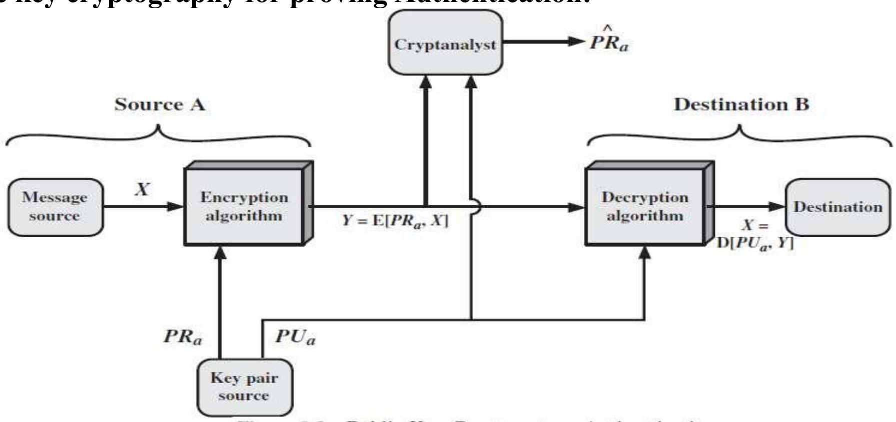


Figure 9.3 Public-Key Cryptosystem: Authentication

The above diagrams show the use of public-key encryption to provide authentication:

$$Y = E(PR_a, X)$$

$$X = D(PU_a, Y)$$

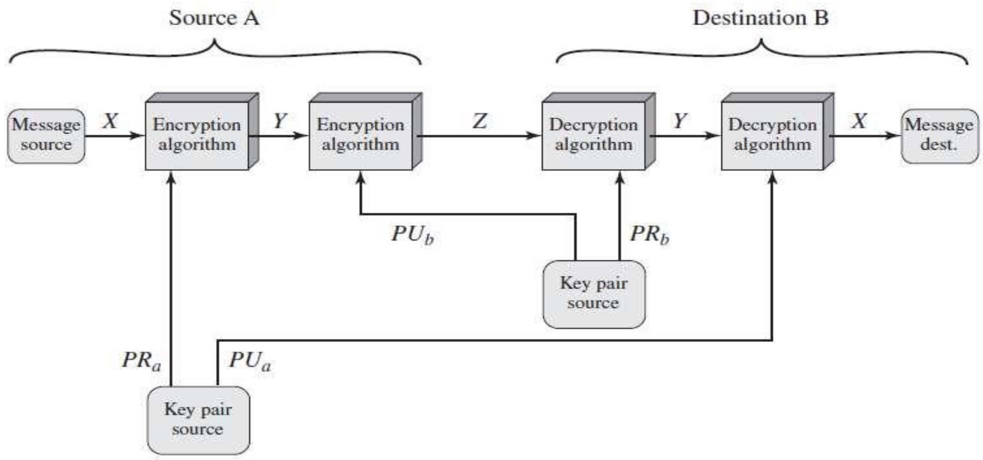
- In this case,A prepares a message to B and encrypts it using A's private key before transmitting it. B can decrypt the message using A's public key. Because the message was encrypted using A's private key, only A could have prepared the message. Therefore, the entire encrypted message serves as a **digital signature.**
- It is impossible to alter the message without access to A's private key, so the message is authenticated both in terms of source and in terms of data integrity.

Public key cryptography for both authentication and confidentiality (Secrecy)

It is, however, possible to provide both the authentication function and confidentiality by a double use of the public-key scheme (above figure):

$$Z = E(PU_b, E(PR_a, X))$$

$$X = D(PU_a, D(PR_b, Z))$$

	 Figure 9.4 Public-Key Cryptosystem: Authentication and Secrecy In this case, we begin as before by encrypting a message, using the sender’s private key. This provides the digital signature. Next, we encrypt again, using the receiver’s public key. The final ciphertext can be decrypted only by the intended receiver, who alone has the matching private key. Thus, confidentiality is provided.			
	b) Explain Four possible approaches to attacking the RSA algorithm c) Four possible approaches to attacking the RSA algorithm are 1. **Brute force:** This involves trying all possible private keys. 2. **Mathematical attacks:** There are several approaches, all equivalent in effort to factoring the product of two primes. 3. **Timing attacks:** These depend on the running time of the decryption algorithm. 4. **Chosen ciphertext attacks:** This type of attack exploits properties of the RSA algorithm.	1+1+1+1 [04]	CO2	L2