Solution and scheme of Internal Assessment Test II – Oct. 2019

| Sub: | Cryptography and Network Security | | | | | Sub Code: | 15TE71 | Branch: | TCE |
|---|---|---|---|---|---|---|---|---|---|
| Date: | 15/10/2019 | Duration: | 90 min's | Max Marks: | 50 | Sem / Sec: | 7th A | | OBE |

1(a) What are the requirements a public key cryptosystem must full fill to be a secure algorithm.

**REQUIREMENTS FOR PUBLIC KEY CRYPTOGRAPHY:** **[5 marks]**

1. It is computationally easy for a party B to generate a pair (public key *PUb*, private key *PRb*).
2. It is computationally easy for a sender A, knowing the public key and the message to be encrypted, *M*, to generate the corresponding ciphertext: *C* = E(*PUb*, *M*)
3. It is computationally easy for the receiver B to decrypt the resulting ciphertext using the private key to recover the original message: *M* = D(*PRb*,*C*) = D[*PRb*, E(*PUb*,*M*)]
4. It is computationally infeasible for an adversary, knowing the public key, *PUb*, to determine the private key, *PRb*.
5. It is computationally infeasible for an adversary, knowing the public key, *PUb*, and a ciphertext, *C*, to recover the original message, *M*. We can add a sixth requirement that, although useful, is not necessary for all public-key applications:
6. The two keys can be applied in either order: *M* = D[*PUb*, E(*PRb*, *M*)] = D[*PRb*, E(*PUb*, *M*)]

1(b) Specify the applications of a public key cryptosystem.

**APPLICATIONS FOR PUBLIC KEY CRYPTOSYSTEMS:** **[5 marks]**

1. Same algorithm is used for encryption and decryption but different keys are used. Depending on the applications, the sender uses either sender's private key or the receiver's public key or both.
2. We can classify the use of public key cryptosystems into 3 categories:
   a) **Encryption/Decryption:** The sender encrypts the message with the receiver's public key.
   b) **Digital Signature:** The sender encrypts the message using its private key.
   c) **Key Exchange:** Two sides co-operate to exchange a session key. Several different approaches are possible, involving the private key(s) of one or both the parties.
3. Some algorithms are suitable for all 3 applications, Where as others can be used only for few applications.

| Algorithm | Encryption/Decryption | Digital Signature | Key Exchange |
|---|---|---|---|
| RSA | Yes | Yes | Yes |
| Elliptic Curve | Yes | Yes | Yes |
| Diffie-Hellman | No | No | Yes |
| DSS | No | Yes | No |

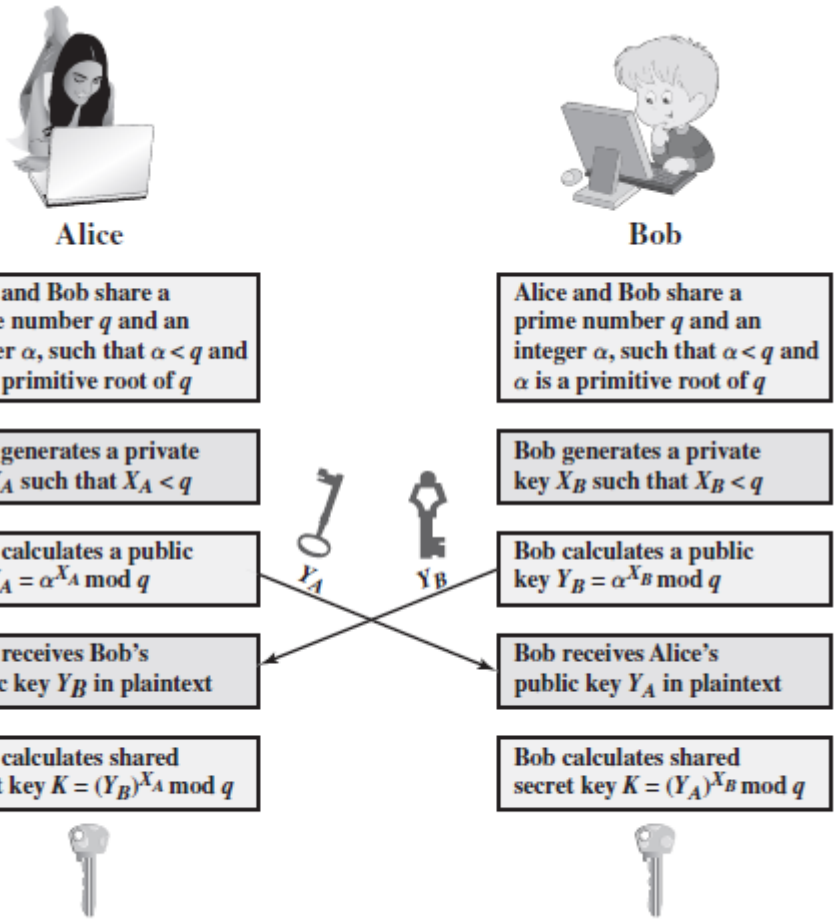
2. Explain the Diffie-Hellman Algorithm in detail.

**Diffie Hellman Key Exchange Algorithm:** **[Description 5 marks]**

1. In this scheme, there are two publicly known numbers those are: a prime number $q$ and an integer $\alpha$ that is a primitive root of $q$.
2. User $A$ selects a random integer $X_A < q$ and compute $Y_A = \alpha^{X_A} \bmod q$.
3. User $B$ selects a random integer $X_B < q$ and compute $Y_B = \alpha^{X_B} \bmod q$.
4. User A computes the key as $K_A = {Y_B}^{X_A} \bmod q$
5. User B computes the key as $K_B = {Y_A}^{X_B} \bmod q$

$K_A = {Y_B}^{X_A} \bmod q$
$K_A = (\alpha^{X_B} \bmod q)^{X_A} \bmod q$
$K_A = (\alpha^{X_B})^{X_A} \bmod q$
$K_A = \alpha^{X_B X_A} \bmod q$
$K_A = (\alpha^{X_A})^{X_B} \bmod q$
$K_A = (\alpha^{X_A} \bmod q)^{X_B} \bmod q$

$K_A = {Y_A}^{X_B} \bmod q$
$K_A = K_B$




The Diffie-Hellman Key Exchange

User $A$ *and* $B$ use Diffie-Hellman algorithm with a prime $q = 71$ and primitive root $\alpha = 7$.
If user $A$ has private key $X_A = 5$, what is $A's$ public key $Y_A = 7^5 \ mod \ 71 = 51$ **[Example 5 marks]**
If user $B$ has private key $X_B = 5$, what is $B's$ public key $Y_B = 7^2 \ mod \ 71 = 49$
The shared secret key $K_A = {Y_B}^{X_A} \ mod \ q \Rightarrow \ K_A = 49^5 \ mod \ 71 = 45$
*and* $K_B = {Y_A}^{X_B} \ mod \ q \Rightarrow \ K_B = 51^2 \ mod \ 71 = 45$

3. In RSA system it is given $p = 17, q = 31, e = 7$ , $M = 2$. Find the cipher text $C$ and also find $M$ from the decryption.

$n = pq = 17 \times 31 = 527$
$\emptyset(n) = (p-1) \times (q-1) = 16 \times 30 = 480$ **[2 marks]**
$e = 7$
$ed \ mod \ \emptyset(n) \equiv 1 \Rightarrow d = \ e^{-1} \ mod \ \emptyset(n) \Rightarrow d = -137 \ mod \ 480 =$ **343** **[2 marks]**

| $q$ | $r_1$ | $r_2$ | $r$ | $t_1$ | $t_2$ | $t = t_1 - qt_2$ |
|---|---|---|---|---|---|---|
| 68 | 480 | 7 | 4 | 0 | 1 | $-68$ |
| 1 | 7 | 4 | 3 | 1 | $-68$ | 69 |
| 1 | 4 | 3 | 1 | $-68$ | 69 | $-137$ |
| 3 | 3 | 1 | 0 | 69 | $-137$ | 480 |
| | 1 | 0 | | **$-137$** | 480 | |

$PU = \{7,527\}$ *and* $PR = \{343,527\}$ **[2 marks]**
$C = M^e \ mod \ n \Rightarrow C = 2^7 mod \ 527 = 128$ **[2 marks]**

$2^7 mod \ 527$
$(7)_{10} = (111)_2$
$1{:}2 \ mod \ 527 = 2$

$1: (2)^2 \times 2 \; mod \; 527 = 8$
$1: (8)^2 \times 2 \; mod \; 527 = 128$

$M = C^d \; mod \; n = 128^{343} \; mod \; 527 = 2$ **[2 *marks*]**

$128^{343} \; mod \; 527$
$(343)_{10} = (101010111)_2$
$1: 128 \; mod \; 527 = 128$
$0: (128)^2 \; mod \; 527 = 47$
$1: (47)^2 \times 128 \; mod \; 527 = 280$
$0: (280)^2 \; mod \; 527 = 404$
$1: (404)^2 \times 128 \; mod \; 527 = 314$
$0: (314)^2 \; mod \; 527 = 47$
$1: (47)^2 \times 128 \; mod \; 527 = 280$
$1: (280)^2 \times 128 \; mod \; 527 = 66$
$1: (66)^2 \times 128 \; mod \; 527 = 2$

4. Define the elliptic curve over $Z_P$. Also write the corresponding addition formula.

**ELLIPTIC CURVE OVER $Z_P$ :** **[5 marks]**

1. Elliptic curve cryptography makes use of elliptic curves in which the variables and coefficients are all restricted to elements of a finite field.
2. Two families of elliptic curves are used in cryptographic applications:
   a) prime curves over $Z_P$
   b) Binary curves over $GF(2^m)$
3. In prime curve over $Z_P$, the variable and co-efficient all take values in the set of integers from $0 \; to \; p-1$
4. In binary curve over $GF(2^m)$, the variable and co-efficient all take values in $GF(2^m)$.
5. Elliptic curve over $Z_P$ is represented as $y^2 mod \; p = (x^3 + ax + b) mod \; p$

**Rules for Addition over $E_P(a, b)$:** **[5 marks]**

1. $P + O = P$
2. If $P = (x_P, y_P)$, *then* $-P = (x_P, -y_P)$ *e.g. P=(13,7) in* $E_{23}(1,1)$ *then* $-P = (13, -7) => -P = (13,16$
3. If $P = (x_P, y_P)$ *and* $Q = (x_Q, y_Q)$ then $R = P + Q = (x_R, y_R)$ is determined by

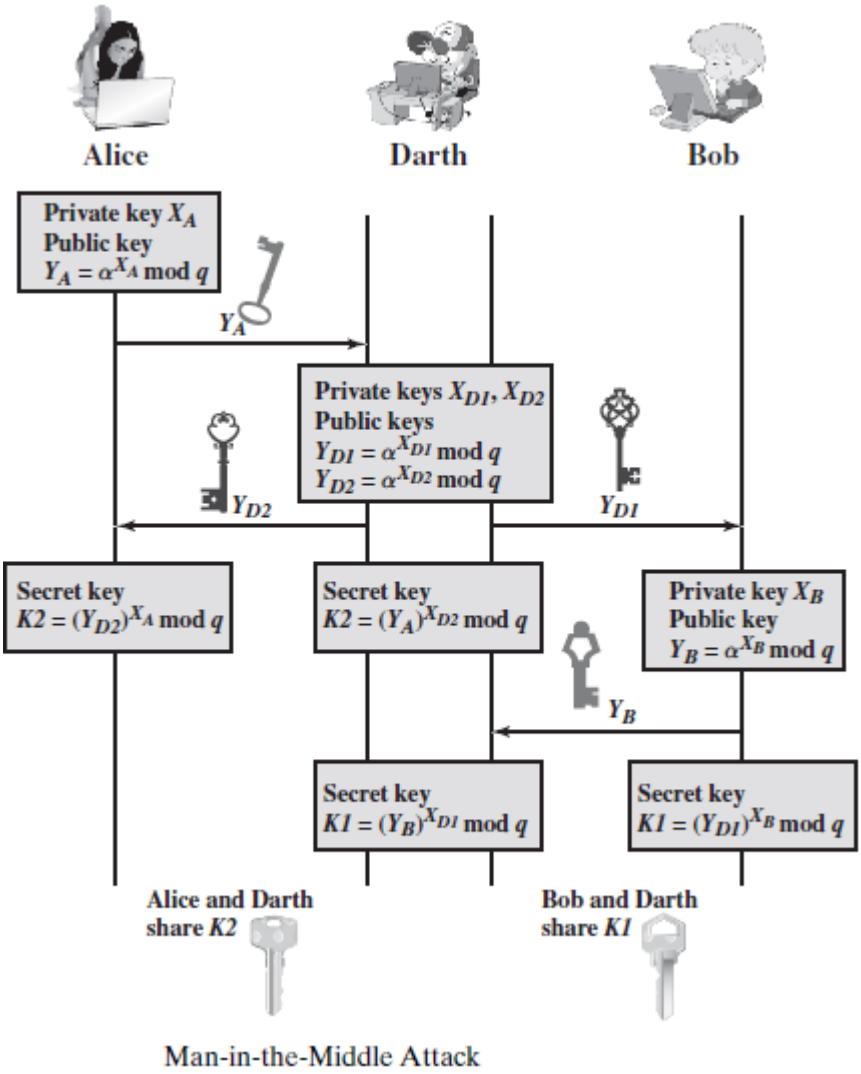
| $If \quad P \neq Q \;\; (i.e. P + Q = R)$ | $If \quad P = Q \;\; (i.e. P + P = 2P)$ |
|---|---|
| $x_R = (\Delta^2 - x_P - x_Q) \; mod \; p$<br>$y_R = (\Delta(x_P - x_R) - y_P) \; mod \; p$<br>$Where \;\; \Delta = \left(\frac{y_Q - y_p}{x_Q - x_P}\right) \; mod \; p$ | $x_R = (\Delta^2 - 2x_P) \; mod \; p$<br>$y_R = (\Delta(x_P - x_R) - y_P) \; mod \; p$<br>$Where \;\; \Delta = \left(\frac{3{x_P}^2 + a}{2y_P}\right) \; mod \; p$ |

4. Multiplication is defined as repeated addition; for example, $4P = P + P + P + P$.

5(a). Explain Man-in-middle attack in detail.

**MAN-IN-MIDDLE ATTACK:** **[Diagram: 2 Marks]**

a) Diffie Hellman Algorithm is insecure against man in middle attack.
b) The attack proceeds as follows:




Man-in-the-Middle Attack **[Explanation: 3 Marks]**

1. Darth prepare for the attack by generating 2 random key $X_{D_1}$ *and* $X_{D_2}$ and computes its corresponding private key $Y_{D_1}$ *and* $Y_{D_2}$.
2. Alice sends $Y_A$ to Bob.
3. Darth intercepts $Y_A$ and transmits $Y_{D_1}$. Darth also calculate the $K_2 = (Y_A)^{X_{D_2}} \ mod \ q$
4. Bob receives $Y_{D_1}$ and calculate $K_1 = \left(Y_{D_1}\right)^{X_B} \ mod \ q$
5. Bob transmits the $Y_B$ to Alice.
6. Darth intercepts $Y_B$ and transmits $Y_{D_2}$ to Alice and Darth calculate $K_1 = (Y_B)^{X_{D_1}} \ mod \ q$
7. Alice receives $Y_{D_2}$ and calculate $K_2 = \left(Y_{D_2}\right)^{X_A} \ mod \ q$

At this point, Bob and Alice think that they share a secret key, but instead Bob and Darth shared secret key $K_1$ and Alice and Darth shared the secret key $K_2$. All the future communication between Bob and Alice is compromised.

5(b). Users A and B use the Diffie-Hellman key exchange technique with a common prime q = 71 and a primitive root α = 7.

i. If user A has private key $X_A = 5$ , what is A's public key $Y_A$?
ii. If user B has private key $X_B = 2$ , what is B's public key $Y_B$?
iii. What is the shared secret key $K_A$ and $K_B$ ?

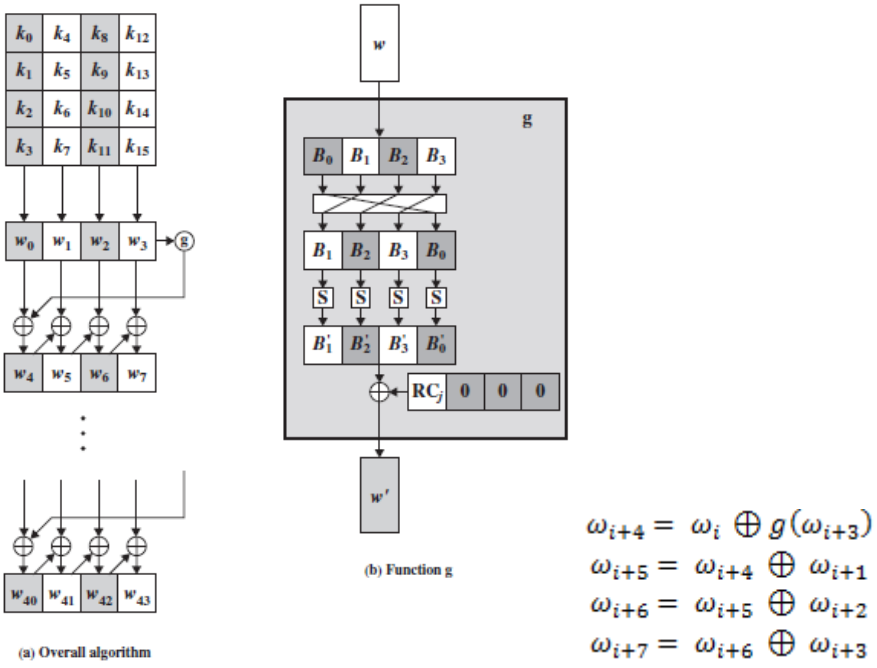
$Y_A = \alpha^{X_A} \ mod \ q \Rightarrow \ Y_A = 7^5 \ mod \ 71 = 51$ **[1 mark]**
$Y_B = \alpha^{X_B} \ mod \ q \Rightarrow \ Y_B = 7^2 \ mod \ 71 = 49$ **[1 mark]**
$K_A = {Y_B}^{X_A} \ mod \ q \Rightarrow \ K_A = 49^5 \ mod \ 71 = 45$ **[1.5 marks]**
$K_B = {Y_A}^{X_B} \ mod \ q \Rightarrow \ K_B = 51^2 \ mod \ 71 = 45$ **[1.5 marks]**
$K_A = K_B = 45$

6. Explain the AES Key generation algorithm with appropriate block diagram

**AES KEY EXPANSION: (Diagram 4 marks + Explain 6 marks)**

**Key Expansion Algorithm:**

1. The AES key expansion algorithm takes as input a four-word (16-byte) key and produces a linear array of 44 words (176 bytes).
2. The key is copied into the first four words of the expanded key.
3. The remainder of the expanded key is filled in four words at a time.
4. Each added word **w**[i] depends on the immediately preceding word, **w**[i - 1], and the word four positions back, **w**[i - 4] and a simple XOR is used
5. For a word whose position in the **w** array is a multiple of 4, a more complex function 'g' is used.
6. The generation of the expanded key, using the symbol g to represent that complex function.
7. The function 'g' consists of the following sub-functions:
   a. Perform a one-byte left circular rotation. This means that an input word [B0, B1, B2, B3] is transformed into [B1, B2, B3, B0].
   b. Perform a byte substitution using the S-box table.
   c. The result of step 1 and step 2 is XORed with a Round Constant RC[j]




$$\omega_{i+4} = \omega_i \oplus g(\omega_{i+3})$$
$$\omega_{i+5} = \omega_{i+4} \oplus \omega_{i+1}$$
$$\omega_{i+6} = \omega_{i+5} \oplus \omega_{i+2}$$
$$\omega_{i+7} = \omega_{i+6} \oplus \omega_{i+3}$$

**Figure: AES Key Expansion**

8. The round constant is a word in which the three rightmost bytes are always 0.

| Rcon Constants (Base 16) | | | |
|---|---|---|---|
| Round | Constant(Rcon) | Round | Constant(Rcon) |
| 1 | 01 00 00 00 | 6 | 20 00 00 00 |
| 2 | 02 00 00 00 | 7 | 40 00 00 00 |
| 3 | 04 00 00 00 | 8 | 80 00 00 00 |
| 4 | 08 00 00 00 | 9 | 1B 00 00 00 |
| 5 | 10 00 00 00 | 10 | 36 00 00 00 |

$$\omega_{i+4} = \omega_i \oplus g(\omega_{i+3})$$
$$\omega_{i+5} = \omega_{i+4} \oplus \omega_{i+1}$$
$$\omega_{i+6} = \omega_{i+5} \oplus \omega_{i+2}$$
$$\omega_{i+7} = \omega_{i+6} \oplus \omega_{i+3}$$

7. Encrypt the plain text "MONDAY" using the Hill cipher with key = $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$. Show your calculation in obtaining cipher text.

Plain Text: MONDAY

$Plain\ Text = \begin{bmatrix} M & N & A \\ O & D & Y \end{bmatrix} = \begin{bmatrix} 12 & 13 & 0 \\ 14 & 3 & 24 \end{bmatrix}$ **(3 marks)**

Key is a 2X2 matrix

$K = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$

$C = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 12 & 13 & 0 \\ 14 & 3 & 24 \end{bmatrix} mod\ 26 = \begin{bmatrix} 164 & 129 & 96 \\ 158 & 86 & 168 \end{bmatrix} mod\ 26$ **(3 marks)**

$C = \begin{bmatrix} 8 & 25 & 18 \\ 2 & 8 & 12 \end{bmatrix}$ **(3 marks)**

$C = \begin{bmatrix} I & Z & S \\ C & I & M \end{bmatrix} = ICZISM$ **(1 mark)**

$K^{-1} = \dfrac{Adj\ [K]}{Det\ [K]}$

$Co - factor\ [K] = \begin{bmatrix} 7 & -5 \\ -4 & 9 \end{bmatrix} \quad Adj\ [K] = \begin{bmatrix} 7 & -4 \\ -5 & 9 \end{bmatrix}$

$Det\ [K] = 43 mod\ 26 = 17$

$\dfrac{1}{17}\ mod\ 26 = 17^{-1}\ mod\ 26$

| $q$ | $r_1$ | $r_2$ | $r$ | $t_1$ | $t_2$ | $t$ |
|---|---|---|---|---|---|---|
| 1 | 26 | 17 | 9 | 0 | 1 | -1 |
| 1 | 17 | 9 | 8 | 1 | -1 | 2 |
| 1 | 9 | 8 | 1 | -1 | 2 | -3 |
| 8 | 8 | 1 | 0 | 2 | -3 | 26 |
| | 1 | 0 | | **-3** | 26 | |

$17^{-1}\ mod\ 26 = -3\ mod\ 26 = 23$

$K^{-1} = 23 \begin{bmatrix} 7 & -4 \\ -5 & 9 \end{bmatrix} = \begin{bmatrix} 161 & -92 \\ -115 & 207 \end{bmatrix} mod 26 = \begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix}$

$M = K^{-1}C = \begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} \begin{bmatrix} 8 & 25 & 18 \\ 2 & 8 & 12 \end{bmatrix} = \begin{bmatrix} 64 & 221 & 234 \\ 170 & 575 & 570 \end{bmatrix} mod\ 26 = \begin{bmatrix} 12 & 13 & 0 \\ 14 & 3 & 24 \end{bmatrix} = \begin{bmatrix} M & N & A \\ O & D & Y \end{bmatrix}$

$M = MONDAY$