CMR INSTITUTE OF TECHNOLOGY

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

Scheme and Solution of Internal Assesment Test – II

Sub:	**Cryptography**		Sec	7 A, B, C, D			Code:	**18EC744**
Date:	**20/12/2021**	Duration:	90 mins	Max Marks:	50	Sem: VII	Branch:	ECE

Solution

1 *Explain the AES encryption and decryption process with a neat diagram.* **[10 marks]**

Ans

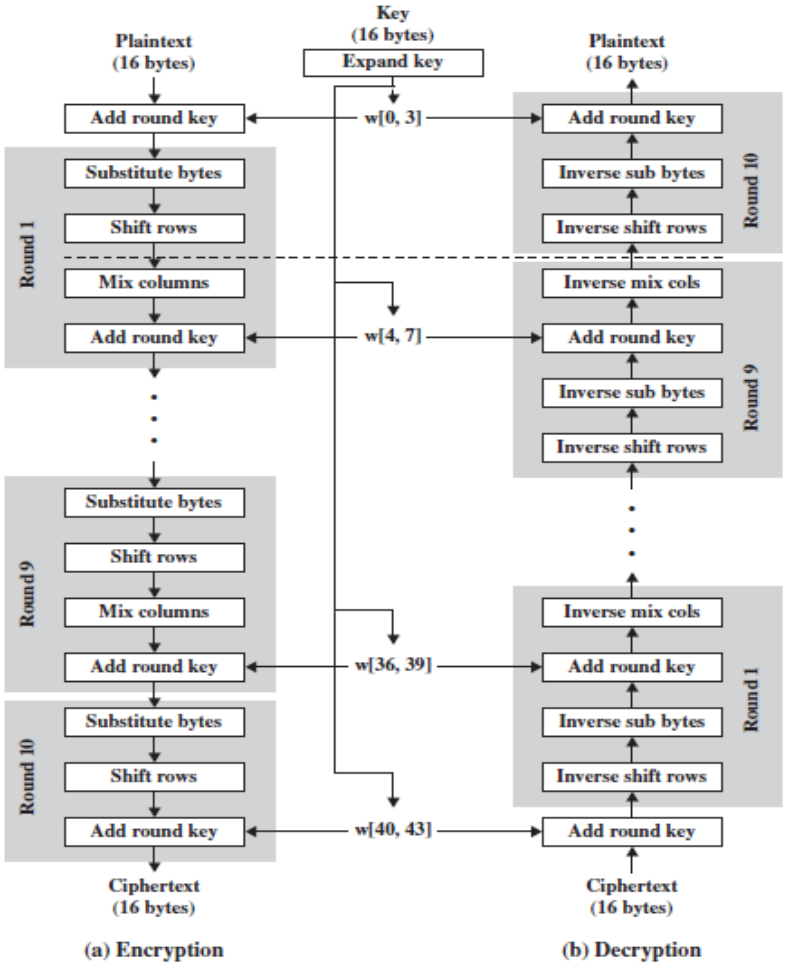


Figure: AES Encryption and Decryption

Diagram [5 marks] + Description [5 marks]

AES doesn't use the Feistel structure. Feistel structure, half of the data block is used to modify the other half of the data block and then the halves are swapped. AES instead processes the entire data block as a single matrix during each round using substitutions and permutation. The key that is provided as input is expanded into an array of forty-four 32-bit words, **w**[*i*]. Four different stages are used, one of permutation and three of substitution:

a) **Substitute bytes:** Uses an S-box to perform a byte-by-byte substitution of the block
b) **ShiftRows:** A simple permutation
c) **MixColumns:** A substitution that makes use of arithmetic over GF(28)
d) **AddRoundKey:** A simple bitwise XOR of the current block with a portion of the expanded key

The cipher begins with an AddRoundKey stage, followed by nine rounds that each includes all four stages, followed by a tenth round of three stages. AddRoundKey stage makes use of the key.The cipher begins and ends with an AddRoundKey stage. Each stage is easily reversible. For the Substitute Byte, ShiftRows, and MixColumns stages, an inverse function is used in the decryption algorithm. For the AddRoundKey stage, the inverse is achieved by XORing the same round key to the block, using the

result that A ⊕ B ⊕ B = A. In AES, the decryption algorithm is not identical to the encryption algorithm.

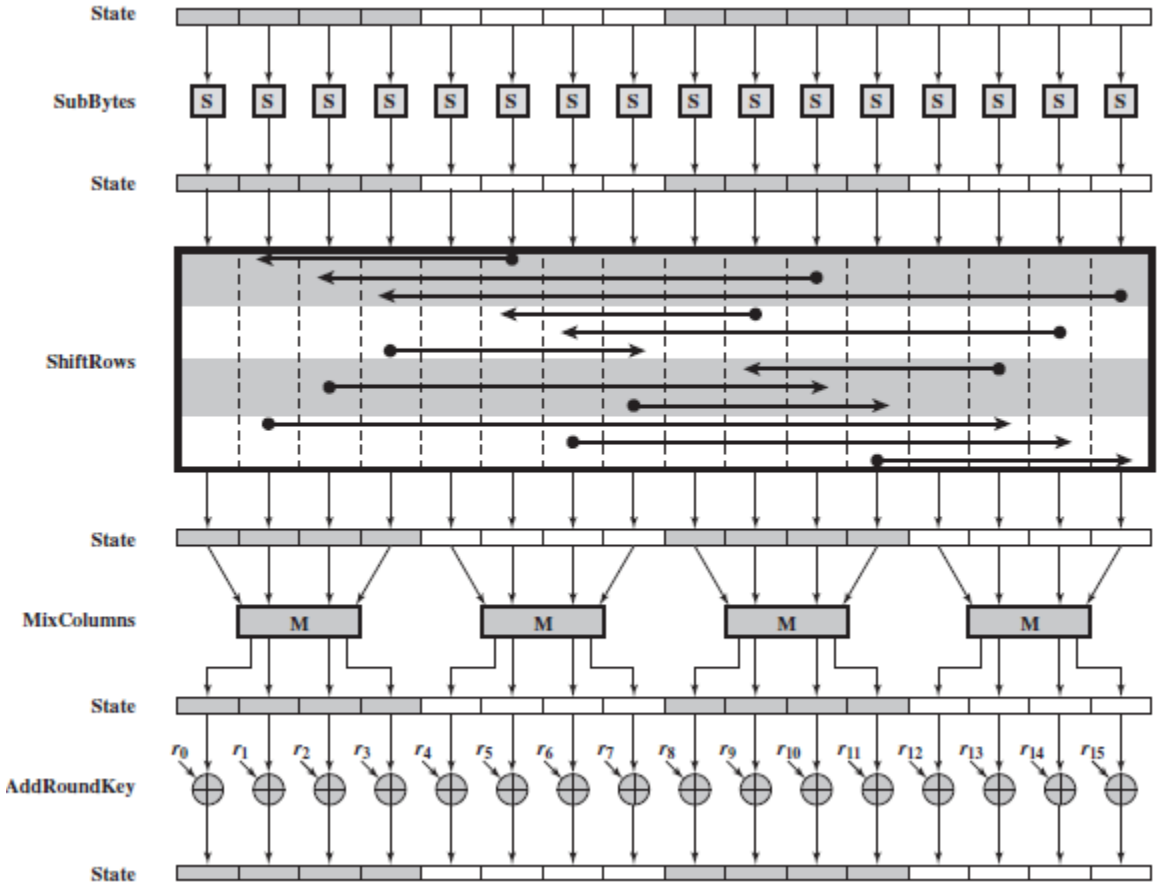


Figure: AES Encryption Round

As all stages are reversible, it is easy to perform decryption to recover the plain text. Encryption and decryption going in opposite vertical directions. The first *N* - 1 rounds consist of four distinct transformation functions:

- SubBytes,
- ShiftRows,
- MixColumns,
- AddRoundKey

The final round contains only three transformations those are SubBytes, ShiftRows and AddRoundKey, and there is an initial single transformation (AddRoundKey) before the first round, which can be considered Round 0.

2 *Define the following with relevant examples:*

(i) Groups, Rings and Fields **[10 marks]**

(ii) Fermat's and Euler's Theorem

Ans **GROUP RING AND FIELDS:**

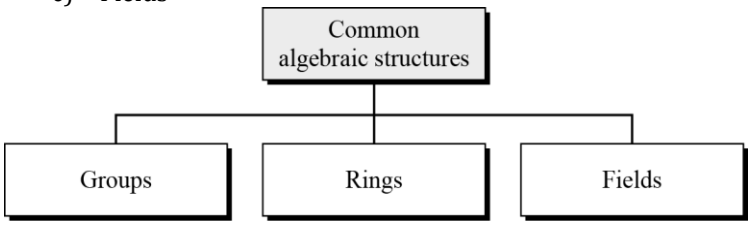
The combination of the set and the operations that are applied to the elements of the set is called an algebraic structure. There are 3 common algebraic structures

a) Group
b) Rings
c) Fields

Group [2 marks]

+

Ring [2 marks]



+

GROUP:

1. A group (G) is a set of elements with a binary operation (•) that satisfies four properties (or axioms). It is denoted as **{*G*, • }**
2. A commutative group is also called abelian group. Abelian group is a group in which the operator satisfies the four properties for group plus an extra property i.e. commutativity property.
3. The 4 properties plus commutativity are defined as follows:

(A1) Closure:	If a and b belong to G, then $a \cdot b$ is also in G.
(A2) Associative:	$a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all a, b, c in G.
(A3) Identity element:	There is an element e in G such that $a \cdot e = e \cdot a = a$ for all a in G.
(A4) Inverse element:	For each a in G, there is an element a' in G such that $a \cdot a' = a' \cdot a = e$.

Abelian Group:

(A5) Commutative:	$a \cdot b = b \cdot a$ for all a, b in G.

RING:

A ring R, sometimes denoted by $\{ R, +, \times \}$is a set of elements with two binary operations, called addition and multiplication, such that for all a, b, c in R the following axioms are obeyed.

(A1–A5)	R is an abelian group with respect to addition; that is, R satisfies axioms A1 through A5. For the case of an additive group, we denote the identity element as 0 and the inverse of a as $-a$.
(M1) Closure under multiplication:	If a and b belong to R, then ab is also in R.
(M2) Associativity of multiplication:	$a(bc) = (ab)c$ for all a, b, c in R.
(M3) Distributive laws:	$a(b + c) = ab + ac$ for all a, b, c in R. $(a + b)c = ac + bc$ for all a, b, c in R.

FIELD:

A **field** F, sometimes denoted by $\{F, +, *\}$, is a set of elements with two binary operations, called *addition* and *multiplication*, such that for all a, b, c in F the following axioms are obeyed.

(A1–A5)	R is an abelian group with respect to addition; that is, R satisfies axioms A1 through A5. For the case of an additive group, we denote the identity element as 0 and the inverse of a as $-a$.
(M1) Closure under multiplication:	If a and b belong to R, then ab is also in R.
(M2) Associativity of multiplication:	$a(bc) = (ab)c$ for all a, b, c in R.
(M3) Distributive laws:	$a(b + c) = ab + ac$ for all a, b, c in R. $(a + b)c = ac + bc$ for all a, b, c in R.
(M4) Commutativity of multiplication:	$ab = ba$ for all a, b in R.
(M5) Multiplicative identity:	There is an element 1 in R such that $a1 = 1a = a$ for all a in R.
(M6) No zero divisors:	If a, b in R and $ab = 0$, then either $a = 0$ or $b = 0$.
(M7) Multiplicative inverse:	For each a in F, except 0, there is an element a^{-1} in F such that $aa^{-1} = (a^{-1})a = 1$.

Fermat's Theorem: Fermat's Theorem and Euler's Theorem are mostly used in public key cryptosystem. Fermat's Theorem and Euler's Theorem are helpful for quickly finding solution to exponentiations. Fermat's theorem has 2 versions of the theorem.

First Version: If 'P' is prime and 'a' is any integer but not divisible by 'P' then

$$a^{P-1} mod\ P = 1$$

Second Version: The second version removes the condition if 'P' is a prime and 'a' is any integer, then

$$a^{P} mod\ P = a$$

Example:

$7^{18} mod\ 19 = 1, \quad 3^{5} mod\ 5 = 3, \quad 10^{5} mod\ 5 = 0$

Euler's Theorem: Euler's theorem can be thought as a generalization of a Fermat's theorem. The modulus in the Fermat's theorem is a prime, but the modulus in Euler's theorem is an integer.
Like Fermat's theorem there are 2 versions of Euler's theorem

Field [2 marks]

+

Fermat's Theorem [2 marks]

+

Euler's Theorem [2 marks]

First Version: If 'a' and 'n' are relatively prime then

$a^{\emptyset(n)} mod\ n = 1$

Second Version: like Fermat's theorem, it removes the condition that 'a' and 'n' should be Co-prime.

$a^{K.\emptyset(n)+1}\ mod\ n = a$

Example:

$20^{62} mod\ 77 = 15, \quad 6^{24} mod\ 35 = 1$

3 *For the group $G = \langle Z_{11}{}^{*}, \times \rangle$* **[10 marks]**

(i) Find the order of the group.

(ii) Find the primitive roots in the group.

(iii) Show that the group is cyclic.

(iv) Make a table of discrete logarithms

Ans (i) The order of the group is 10 as the elements are $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. **[2 marks] +**

(ii) The generators are: 2, 6, 7 and 8 **[2 marks] +**

$1^0\ mod\ 11 = 1$

$2^0\ mod\ 11 = 1$
$2^1\ mod\ 11 = 2$
$2^2\ mod\ 11 = 4$
$2^3\ mod\ 11 = 8$
$2^4\ mod\ 11 = 5$
$2^5\ mod\ 11 = 10$
$2^6\ mod\ 11 = 9$
$2^7\ mod\ 11 = 7$
$2^8\ mod\ 11 = 3$
$2^9\ mod\ 11 = 6$
$2^{10}\ mod\ 11 = 1$

$3^0\ mod\ 11 = 1$
$3^1\ mod\ 11 = 3$
$3^2\ mod\ 11 = 9$
$3^3\ mod\ 11 = 5$
$3^4\ mod\ 11 = 4$
$3^5\ mod\ 11 = 1$

$4^0\ mod\ 11 = 1$
$4^1\ mod\ 11 = 4$
$4^2\ mod\ 11 = 5$
$4^3\ mod\ 11 = 9$
$4^4\ mod\ 11 = 3$
$4^5\ mod\ 11 = 1$

$5^0\ mod\ 11 = 1$
$5^1\ mod\ 11 = 5$
$5^2\ mod\ 11 = 3$
$5^3\ mod\ 11 = 4$
$5^4\ mod\ 11 = 9$
$5^5\ mod\ 11 = 1$

$6^0\ mod\ 11 = 1$
$6^1\ mod\ 11 = 6$
$6^2\ mod\ 11 = 3$
$6^3\ mod\ 11 = 7$
$6^4\ mod\ 11 = 9$
$6^5\ mod\ 11 = 10$
$6^6\ mod\ 11 = 5$
$6^7\ mod\ 11 = 8$
$6^8\ mod\ 11 = 4$
$6^9 mod\ 11 = 2$
$6^{10}\ mod\ 11 = 1$

$7^0\ mod\ 11 = 1$
$7^1\ mod\ 11 = 7$
$7^2\ mod\ 11 = 5$
$7^3\ mod\ 11 = 2$
$7^4\ mod\ 11 = 3$
$7^5\ mod\ 11 = 10$
$7^6\ mod\ 11 = 4$
$7^7\ mod\ 11 = 6$
$7^8\ mod\ 11 = 9$
$7^9\ mod\ 11 = 8$
$7^{10}\ mod\ 11 = 1$

$8^0\ mod\ 11 = 1$
$8^1\ mod\ 11 = 8$
$8^2\ mod\ 11 = 9$
$8^3\ mod\ 11 = 6$
$8^4\ mod\ 11 = 4$
$8^5\ mod\ 11 = 10$
$8^6\ mod\ 11 = 3$
$8^7\ mod\ 11 = 2$
$8^8\ mod\ 11 = 5$
$8^9\ mod\ 11 = 7$
$8^{10}\ mod\ 11 = 1$

[3 marks] +

$9^0 mod\ 11 = 1$
$9^1\ mod\ 11 = 9$
$9^2\ mod\ 11 = 4$
$9^3\ mod\ 11 = 3$
$9^4\ mod\ 11 = 5$
$9^5\ mod\ 11 = 1$

$10^0\ mod\ 11 = 1$
$10^1\ mod\ 11 = 10$
$10^2\ mod\ 11 = 1$

(iii) The discrete logarithm table is: **[3 marks]**

a	a^1	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}
1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	5	10	9	7	3	6	1
3	3	9	5	4	1	3	9	5	4	1
4	4	5	9	3	1	4	5	9	3	1
5	5	3	4	9	1	5	3	4	9	1
6	6	3	7	9	10	5	8	4	2	1
7	7	5	2	3	10	4	6	9	8	1
8	8	9	6	4	10	3	2	5	7	1
9	9	4	3	5	1	9	4	3	5	1
10	10	1	10	1	10	1	10	1	10	1

4 *Construct the finite field $GF(2^2)$ addition and multiplication table using the polynomial arithmetic modulo $(x^2 + x + 1)$, show the calculation steps.* **[10 marks]**

Ans $GF(2^2) = \{0, 1, x, (x+1)\}$ *and operations are* $[+, \times]$

With irreducible polynomial $(x^2 + x + 1)$

$+$	0	1	x	$(x+1)$
0	0	1	x	$(x+1)$
1	1	0	$(x+1)$	x
x	x	$(x+1)$	0	1
$(x+1)$	$(x+1)$	x	1	0

Addition table [5 marks]

+

$\times$	0	1	x	$(x+1)$
0	0	0	0	0
1	0	1	x	$(x+1)$
x	0	x	$(x+1)$	1
$(x+1)$	0	$(x+1)$	1	x

Multiplication table [5 marks]

5 *Find the inverse of $(x^7 + x + 1)$ in $GF(2^8)$ using the irreducible polynomial $(x^8 + x^4 + x^3 + x + 1)$* **[10 marks]**

Ans

q	r_1	r_2	r	t_1	t_2	$t = t_1 - qt_2$
x	$x^8 + x^4 + x^3 + x + 1$	$x^7 + x + 1$	$x^4 + x^3 + x^2 + 1$	0	1	x
$x^3 + x^2 + 1$	$x^7 + x + 1$	$x^4 + x^3 + x^2 + 1$	x	1	x	$x^4 + x^3 + x + 1$
$x^3 + x^2 + x$	$x^4 + x^3 + x^2 + 1$	x	1	x	$x^4 + x^3 + x + 1$	x^7
x	x	1	0	$x^4 + x^3 + x + 1$	x^7	$x^8 + x^4 + x^3 + x + 1$
	1	0		x^7	$x^8 + x^4 + x^3 + x + 1$	

Solution [10 marks]

The inverse of $(x^7 + x + 1)$ is $(x^7 + x + 1)$under mod $(x^8 + x^4 + x^3 + x + 1)$

4 *Explain steps involved in encryption and decryption of a message using RSA algorithm. Given $p = 17, q = 31, M = 2$ and $e = 7$. Use RSA algorithm to find $n, \emptyset(n), d$ and Cipher text. Also find the message M from decryption.* **[10 marks]**

Ans

Key Generation by Alice	
Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calcuate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} \pmod{\phi(n)}$
Public key	$PU = \{e, n\}$
Private key	$PR = \{d, n\}$

Encryption by Bob with Alice's Public Key	
Plaintext:	$M < n$
Ciphertext:	$C = M^e \bmod n$

Decryption by Alice with Alice's Public Key	
Ciphertext:	C
Plaintext:	$M = C^d \bmod n$

Algorithm [5 marks]

+

Numerical [5 marks]

The RSA Algorithm

$n = pq = 17 \times 31 = 527$

$\emptyset(n) = (p-1) \times (q-1) = 16 \times 30 = 480$

$e = 7$

$ed \ mod \ \emptyset(n) \equiv 1 \Rightarrow d = e^{-1} \ mod \ \emptyset(n) \Rightarrow d = -137 \ mod \ 480 = \mathbf{343}$

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	

$PU = \{7,527\} \ \ and \ \ PR = \{343,527\}$

$C = M^e \ mod \ n \Rightarrow C = 2^7 mod \ 527 = 128$

$2^7 mod \ 527$
$(7)_{10} = (111)_2$
$1: 2 \ mod \ 527 = 2$
$1: (2)^2 \times 2 \ mod \ 527 = 8$
$1: (8)^2 \times 2 \ mod \ 527 = 128$

$M = C^d \ mod \ n = 128^{343} \ mod \ 527 = 2$

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

7 *Explain all possible attacking approach on RSA algorithm.* **[10 marks]**

Ans There are 5 possible approaches to attack the RSA algorithms. Those are:

a) Brute-Force attack
b) Mathematical Attack
c) Timing Attack
d) Hardware Fault based Attack
e) Chosen Cipher text attack

a) **<u>Brute-Force attack:</u>** This means trying with all possible private keys. The defence against the brute force approach is similar like other algorithm i.e. to use a larger key size. But larger key size slower the system as the encryption/ decryption are complex.

b) **<u>Mathematical Attack:</u>** There are 3 approaches to attack RSA mathematically

(i) Factor $'n'$ into its 2 prime factors. This enables calculating $\emptyset(n) = (p-1) \times (q-1)$, which in turn enables determination of $d = e^{-1} \ mod \ \emptyset(n)$

(ii) Determine $\emptyset(n)$ directly, without first determining $p \ and \ q$, which enables determination of $d = e^{-1} \ mod \ \emptyset(n)$

(iii) Determine d directly, without first determining $\emptyset(n)$

For a large $'n'$ with large prime factors, factoring is a hard problem, but it is not as hard as it used to be.

<u>History:</u>

a) In 1977 the 3 inventors of RSA gave one challenge to decode a cipher, they printed in Mertine Gardner's 'Mathematical Game" Column. They offered $100 rewards for the return of a plaintext sentence. In April 1994, a group claimed the prize after only 8 months of work.
b) Now a day's these factorization can be done using
   (i) General Number Field Sieve (GNFS)
   (ii) Special Number Field Sieve (SNFS)
c) Thus we need to be careful in choosing a key size for RSA
d) The team that produced the 768-bit factorization made the following observation:
   (i) Factoring a 1024 bit RSA modulus would be thousand times harder than factorizing a 768 bit modulus. Hence 1024 bit RSA can be used for another

three to four years.

(ii) They suggested few points to avoid the value of $'n'$ being factorized more easily.
A) $p\ and\ q$ should differ in length but only few digits.
B) Both $(p-1)\ \ and\ (q-1)$ contains a large prime factor.
C) $GCD(p-1, q-1)$ should be small.

c) Timing Attack:

(i) Paul Kocher, a cryptographic consultant, demonstrated that a cryptanalyst can determine a private key by keeping track of how long a computer takes to decipher the message.

(ii) It has been observed that processing '1' takes longer time than '0'. Hence like fashion the entire key can be predicted.

(iii) Though timing attack is a serious threat, this can be counter measured in the following ways.
1) Constant Exponentiation Time: Ensure it takes same amount of time. This is a simple fix but degrades the performance
2) Random Delay: a random delay is added to confuse the timing attack.
3) Blinding: Multiply the cipher text by a random number before performing the exponentiation.

d) Hardware Fault based Attack: In this method, the attacker includes faults in the signature computation by reducing the power of the processor. This fault causes the software to produce invalid signatures, which can then be analysed by the attacker to recover the private key. This type of attack is not considered as a serious threat to RSA, because it requires that the attacker should have physical access to the target machine.

e) Chosen Cipher text attack

(i) RSA Algorithm is more vulnerable to chosen cipher text attack (CCA).

(ii) As we know in chosen cipher text attack, the cryptanalyst can choose the number of cipher text and get it decrypted with the target's private key. Means, the cryptanalyst can select a plaintext and find the cipher text using target's public key and then able to get the same plaintext back.

(iii) It is clearly observed, the cryptanalyst doesn't get any new information but it exploits the properties of RSA. It can be better explained with an example:
$E(PU, M_1) \times E(PU\ , M_2) = E(PU, [M_1 \times M_2])$
$Compute\ X = (C \times 2^e) mod\ n$
$X\ is\ a\ chosen\ cipher\ text\ and\ receive\ back\ Y = X^d\ mod\ n$
$X = (C\ mod\ n) \times (2^e\ mod\ n) = (M^e\ mod\ n) \times (2^e\ mod\ n) = (2M)^e\ mod\ n$
Hence from $2M$ it is easy to deduce M

(iv) To overcome this optimal asymmetric encryption padding (OAEP) is used. In this method, the message to be encrypted is padded.