SVKM'S
NMIMS
Deemed to be UNIVERSITY

SUPERVISOR'S SIGNATURE WITH DATE

DATE : 16/9/14

ROLL NO A059

NAME : Chinmay Bhatt TRIMESTER/SEMESTER : 7 DIVISION : A

PROGRAMME : BTech.

SPECIALISATION IT

MODULE (SUBJECT) IS

TOTAL NO. OF SUPPLEMENTARY SHEETS ONLY —

QUESTION NOS.	1	2	3	4	5	6	7	8	9	10	11	12	TOTAL MARKS OBTAINED	MAXIMUM MARKS
(MARKS OBTAINED) (TO BE FILLED IN BY EXAMINER)	03	03	05										11	15

SIGNATURE OF THE EXAMINER

INSTRUCTIONS TO BE STRICTLY FOLLOWED BY CANDIDATES

1. This answer-book contains eight pages. Check whether the relevant answer-book provided contains eight pages and whether the pages are properly numbered.
2. Candidates should occupy the correct seats as per the seating plan displayed and write appropriate details in the space provided for the purpose on the answer book.
3. Candidates must produce their photo identity card provided by the University for verification to the room supervisor during the examination. Candidates will not be permitted to appear for the examination without the identity card.
4. As per rules, Candidates, who are not in their seats by the time notified, will not be permitted to appear for the examination.
5. Candidates should ensure that all answer-books including supplementary sheets provided to them bear the signature of the room supervisor and date of examination without which the answer-book will not be examined.
6. Tie all supplementary sheets to the main answer-book relating to the same paper and enter on the first page of the answer-book only the total number of supplementary sheets tied together.

3) $n, g = 17, 11$

Alice choose a random number x
let x be $= 3$

Bob Chooses a random number y
let y be $= 5$

$A = g^x \bmod n$
$B = g^y \bmod n$

$\therefore A = 11^5 \bmod 17$
$B = 11^5 \bmod 17$

$A = 1331 \bmod 17$
$B = 161,051 \bmod 17$

$A = 5$
$B = 10$

Alice sends Bob 'A'
BoB sends Alice 'B'

Alice computes $K1 = B^x \bmod n$
Bob computes $K2 = A^y \bmod n$
$\therefore K1 = 10^3 \bmod 17$
$K2 = 05^5 \bmod 17$

$K1 = 14$
$K2 = 14$

05

Hence Alice and Bob generated a secret symmetric

Question Nos | Marks Awarded

1] a] Masquerading → Active

It a type of identity theft, where the attacker disguises himself as a trusted client or server in order to gain access or steal credentials. Active due to the fact the attacker actively behaves in disguise.

b] Denial of Service → Active

The attacker or attackers actively flood a server or network to prevent legit users from accessing services provided. It can be done by physically plugging out a n/w wire or overloading server with connection requests.

c] Snooping → Passive

The attacker only monitors packets on the network to either gain knowledge about the n/w and n/w devices or to crack n/w password.

d] Traffic Analysis → Passive

Monitoring of N/w traffic, to figure out protocols, encryption methods, hosts, and other activities, usually also used for defensive purposes.

03

Question Nos		Marks Awarded
2]	Disadvantages of fingerprint recognition.	

1] Optical fingerprint scanners have high FRR (False Rejection Rate) which means authorized people are not authenticated properly

2] Residues on the scanner lead to higher FRR

3] Easily damaged.

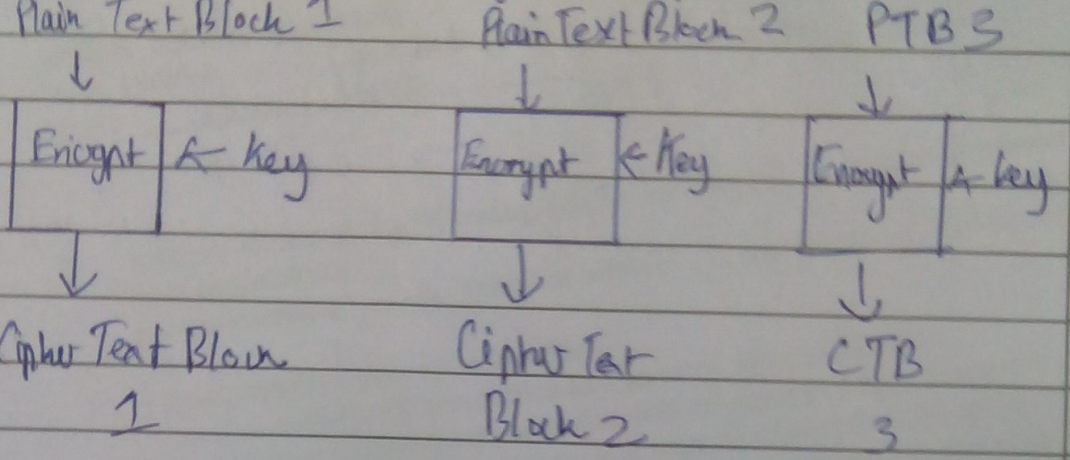
By using a capacitive fingerprint scanner, we can lower FRR, its highly durable and easily cleaned.

03

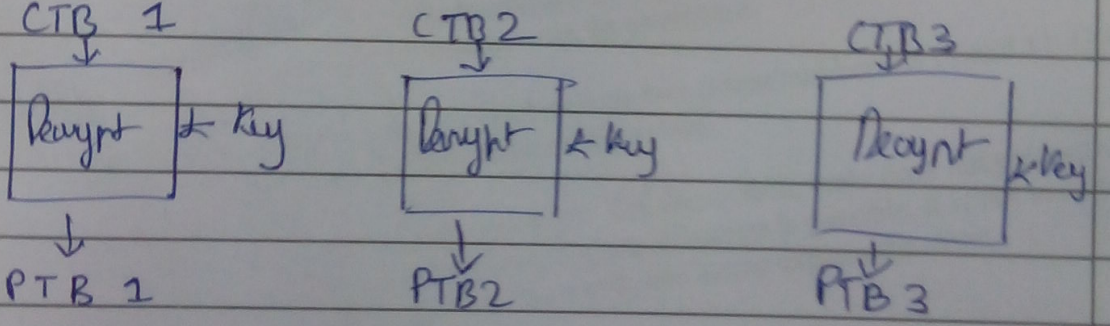
Question Nos | Marks Awarded

3] ECB, Electronic Code Book

Encryption process



Decryption



05

Hence blocks can be encrypted and decrypted in parallel.

Its prone to ~~cryptical analysis~~ analysis attack, if messages are large hence only used for one block transmission.

03

Question Nos

2] Token based authentication.

It is like a challenge response type authentication,
Where client is asked to either provide a number numeric token or a bunch collection of data known as a token.

Tokens can be generated
1] Time based
2] Seed based
3] One-time generation.

Time based, every 60 seconds the client & server generates a new token.

Seed Based, Client & server use the same seed to generate tokens, which are the same.

One time generation -
Server generates tokens, hands them to client, per use the token is discarded.

03