Evaluation Form

ANNA UNIVERSITY

CHENNAI – 25

Nov/Dec 2020 Re-Examination/Apr-May 2021 Regular Examination

Roll No: 2 0 1 8 5 0 6 0 3 4

Name : Gowri S

Programme &Branch : B.Tech / Information Technology

Date of Exam : 23/8/2021 Session: FN/AN;

Subject Code: IT7601 Subject Title: Information Security

Soft Copy Submission (strike-out whichever is not applicable): Microsoft-Teams/~~Email/Google forms~~

PART – A			PART – B & C							Grand Total (in words)
Question No.	✓	Marks	Question No.		✓	(i) Marks	(ii) Marks	(iii) Marks	Total Marks	
1	✓		11	a						
2	✓			b	✓					
3	✓		12	a						
4	✓			b	✓					
5	✓		13	a						
6	✓			b	✓					
7	✓		14	a	✓					
8	✓			b						
9	✓		15	a	✓					Grand Total:
10	✓			b						
			16		✓					
Total										

Declaration by the Examiner: Verified that all the questions attended by the student are valued and the total is found to be correct

Date	Name of the Examiner	Signature of the Examiner

SUBJECT : Information Security
SUBJECT CODE: IT 7601

NAME: Gowri S.
REGNUM: 2018506034

PART-B

(11) (b) Hill Cipher:

Plain Text = "healtheworld"

DIAGRAMS: HEA LTH EWO RLD

$$\begin{pmatrix}7\\4\\0\end{pmatrix}\ \begin{pmatrix}11\\19\\7\end{pmatrix}\ \begin{pmatrix}4\\22\\14\end{pmatrix}\ \begin{pmatrix}17\\11\\3\end{pmatrix}$$

KEY:
$$\begin{pmatrix}2&4&5\\9&2&1\\3&17&7\end{pmatrix}$$

Encryption of Hill Cipher:

$$C = K * P$$

$$\begin{pmatrix}2&4&5\\9&2&1\\3&17&7\end{pmatrix}\begin{pmatrix}7\\4\\0\end{pmatrix} = \begin{pmatrix}30\\71\\89\end{pmatrix} \bmod 26 = \begin{pmatrix}4\\19\\11\end{pmatrix} = \begin{pmatrix}E\\T\\L\end{pmatrix}$$

$$\begin{pmatrix}2&4&5\\9&2&1\\3&17&7\end{pmatrix}\begin{pmatrix}11\\19\\7\end{pmatrix} = \begin{pmatrix}133\\144\\405\end{pmatrix} \bmod 26 = \begin{pmatrix}3\\14\\15\end{pmatrix} = \begin{pmatrix}D\\O\\P\end{pmatrix}$$

$$\begin{pmatrix}2&4&5\\9&2&1\\3&17&7\end{pmatrix}\begin{pmatrix}4\\22\\14\end{pmatrix} = \begin{pmatrix}166\\94\\484\end{pmatrix} \bmod 26 = \begin{pmatrix}10\\16\\16\end{pmatrix} = \begin{pmatrix}K\\Q\\Q\end{pmatrix}$$

$$\begin{pmatrix}2&4&5\\9&2&1\\3&17&7\end{pmatrix}\begin{pmatrix}17\\11\\3\end{pmatrix} = \begin{pmatrix}93\\178\\259\end{pmatrix} \bmod 26 = \begin{pmatrix}15\\22\\25\end{pmatrix} = \begin{pmatrix}P\\W\\Z\end{pmatrix}$$

Encrypted text = ETLDOPKQQPWZ

DATE : 23/8/21

PAGE: 1

Signature S.Gowri

(11) Fermat's theorem:

If p is prime, a is integer such that p does not divide a, then a^{p-1} is congruent to 1 mod p.

$$a^{p-1} \equiv 1 \bmod p$$

If p is prime, a is integer, then

$$a \bmod p \equiv a \bmod p \quad [\because a^{p-1} \equiv 1 \bmod p]$$

APPLICATIONS:

(1) Multiplicative inverse using Fermat's theorem :-

If p is prime, a is integer such that p does not divide a, then $a^{-1} \bmod p \equiv a^{p-2} \bmod p$

Proof

$$aa^{-1} \equiv 1 \bmod p$$

$$aa^{-1} \bmod p \equiv aa^{p-2} \bmod p$$

$$\equiv aa^{-1}a^{p-1} \bmod p \quad \text{(Using Fermat's theorem)}$$

$$= aa^{-1}$$

(2) Used in public key cryptography
(3) Factoring numbers
(4) Decimal Expansions
(5) Primality Testing
(6) Important is elementary number theory

(15)
(a) OWASP top vulnerabilities :-

① Injection :

Injection flaws, such as SQL, NoSQL, OS and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query.

The attacker's hostile data can be the trick the interpreter into executing unintended commands or accessing data without proper authorisation

PREVENTION:

SQL data combine code and data

=> SEPERATE DATA AND CODE

* Parameterize your queries
* Validate which data can be entered
* Escape special characters.

Example: ① Vulnerable SQL call

```
String q = "SELECT * FROM accounts WHERE
    custID = '" + request.getParameter("id") + "'";
```

② Attacker modifies the 'id' parameter in their browser to send code. For example

http://example.com/app/accountView?id='or '1'='1

② BROKEN AUTHENTICATION:

Application function related to authentication and session management are often implemented incorrectly, allowing attackers attackers to compromise passwords, keys, or sessions tokens or to exploit other implementation flaws to assume other user's identities temperorily or permanently.

→ Weak Session Management.
→ Credential stuffing
→ Brute force.
→ Forgotten password.
→ No multi factor authentication.
→ Session don't expire

PREVENTION:

→ Use good authentication libraries
→ Use MFA
→ Enforce strong passwords.
→ Detect and prevent brute force or stuffing attacks.

Example:

Credential stuffing - attackers use lists of known passwords and try them sequentially to gain access. Without automated threat or credential stuffing protection, the application is used by

attackers as a validation mechanism for any password then they

Password-based attacks - web applications relying only on passwords have inherently weak authentication mechanisms, even if passwords have complexity requirements and are rotated. Organisations should switch to multi-factor authentication

③ Sensitive data Exposure :

Many web applications and API's do not properly protect sensitive data, such as financial, healthcare and PII.

Attackers may steal or modify such weakly protected data to conduct credit card fraud identity theft or other crimes. Sensitive data may be compromised without extra protection such as encryption at rest or in transit and requires special precautions when exchanged with the browser

- → Clear-text data transfer
- → Unencrypted storage
- → Weak crypto or key
- → Certificates not validated
- → Exposing PII or credit card.

Example:

No TLS → if a website does not use SSL/TLS for all pages, an attacker can monitor traffic, downgrade connections from HTTPS to HTTP and steal the session cookie

Unsalted hashes - a web application's password database can use unsalted or simple hashes to store passwords.

④ XML External Entities : (XXE)

Many older or poorly configured XML processors elevate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution and denial of service attacks.

Application allows accessing sensitive resources, command execution, recon or cause denial of service

Eg: <!ENTITY xxe SYSTEM "https://192.168.1.1/private">]>

14 (a)

Vulnerability :

→ Security flow

→ Failure of security policies, procedures and controls that allow a subject to commit an action that violates the security policy.

NRL Taxonomy :

The goals of NRL Taxonomy are,

→ To determine how flaws entered system

→ To determine when flows entered systems

→ To determine where flaws are manifested on the system.

The three different schema used are :

→ Genesis of flaws

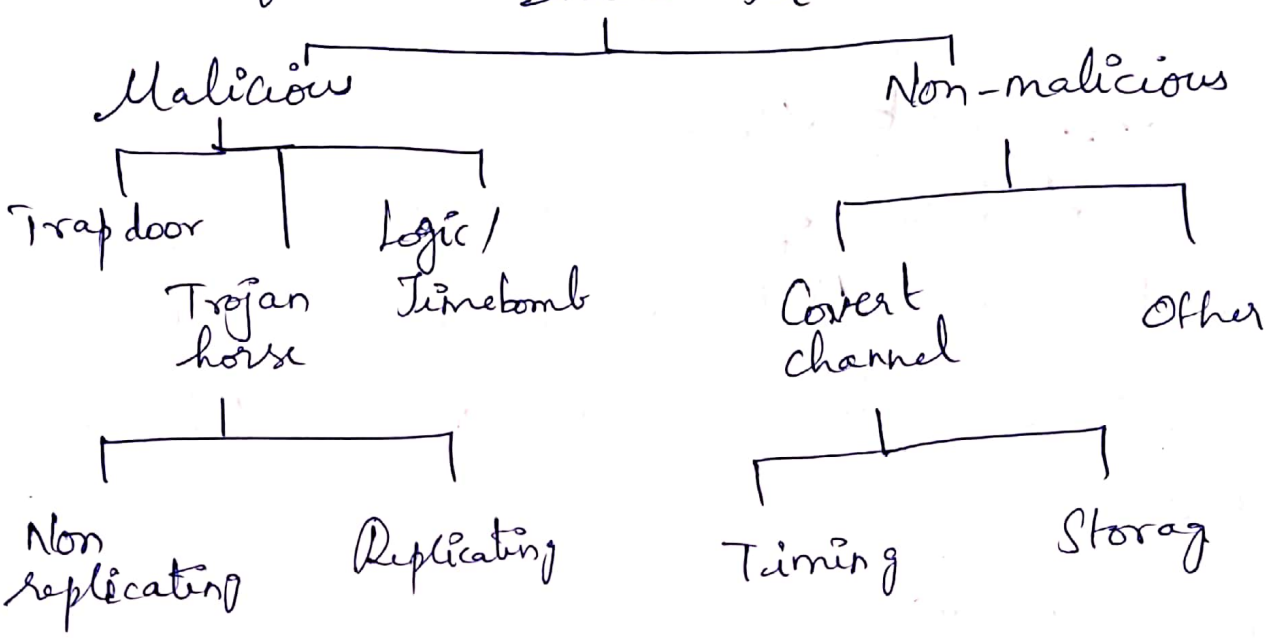
→ Time of flaws

→ Location of flaws

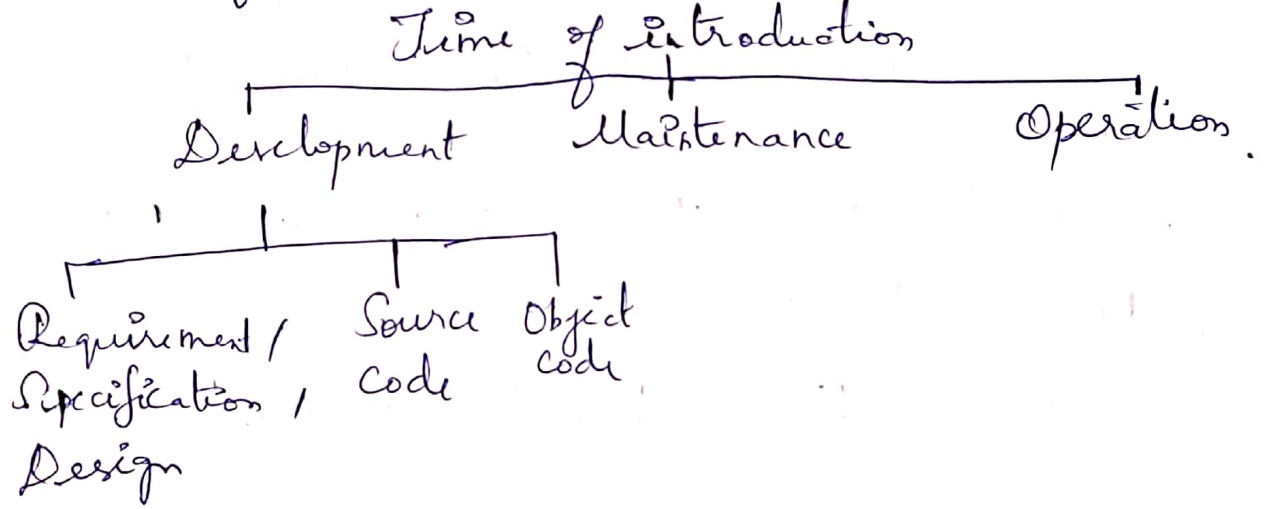
Genesis of Flaws

PTO

Genesis of Flaws:



Time of flaws:



Development Phase:

All activities up to release of initial version of software.

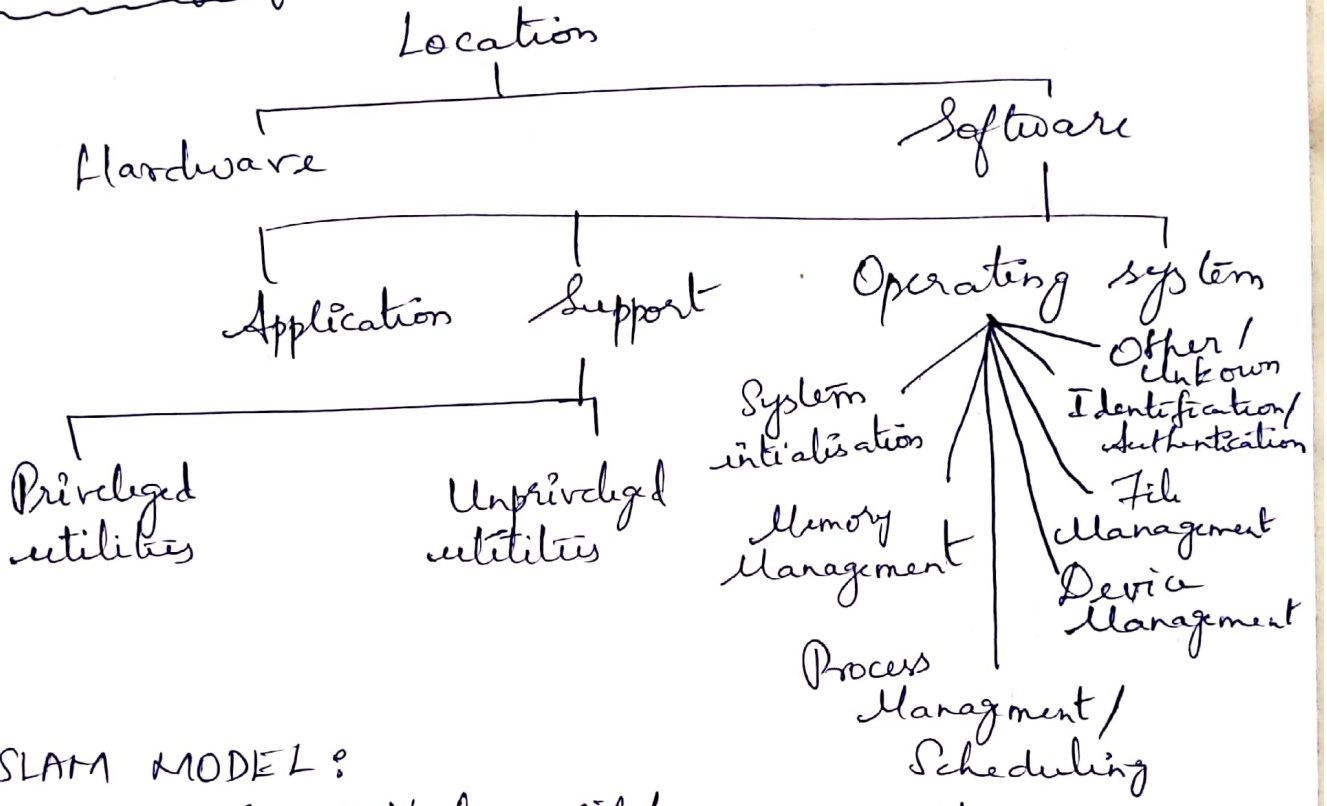
Maintenance Phase:

All activities leading to changes in software performed under configuration control

Operation Phase :

All activities involving patching and not under configuration control

Location of flaws:



ASLAM MODEL :

* Goal : Treat Vulnerabilities as faults and develop scheme based on fault trees

* Focusses specifically on UNIX flaws.

* Classifications unique and unambiguous.

→ Organised as binary tree with a question at each node. Answer determins which branch you take.

→ Leaf node gives classification

* Suited for organising flaws in a database.

Coding faults:

*Introduced during software developed.

* Synchronisation error: Improper serialisation of operations, timing window between two operations creats flaw.

* Condition validation error: Bound not checked, access rights ignored, input not validated, authentication and identification fails

Emergent faults:

* Result from incorrect initialisation, use of application.

* Configuration error: Program installed incorrectly.

* Environment faults: Faults introduced by environment.

(13) (b) Pretty Good Privacy (PGP)

PGP was designed to provide all four aspects of security is privacy, integrity, authentication and non-repudiation in the sending of email

* PGP uses a digital signature (a combination of hashing and public key encryption) to provide integrity, authentication and non-repudiation. It uses the digital signature to provide privacy. The digital signature uses on hash function, one secret key and two private public keys pairs.

* PGP is an open source and freely available software package for email security.

* It provides authentication through the use of Digital signature.

* It provides confidentiality through the use of symmetric block encryption.

* It provides compression by using ZIP algorithm and EMAIL compatability using the radix x64 encoding scheme.

STEPS TO SHOW PGP USER HASHING AND COMBINATION OF THREE KEYS TO GENERATE THE ORIGINAL MESSAGE:

→ The receiver receives the combination of encrypted

secret key and message digest is received.

* The encrypted secret key is decrypted by using the receiver's private key to get the one-time secret key.

* The secret key is then used to decrypt the combination of message and digest.

* The digest is decrypted by using the sender's public key, and the original message is hashed by using a hash function to create a digest.

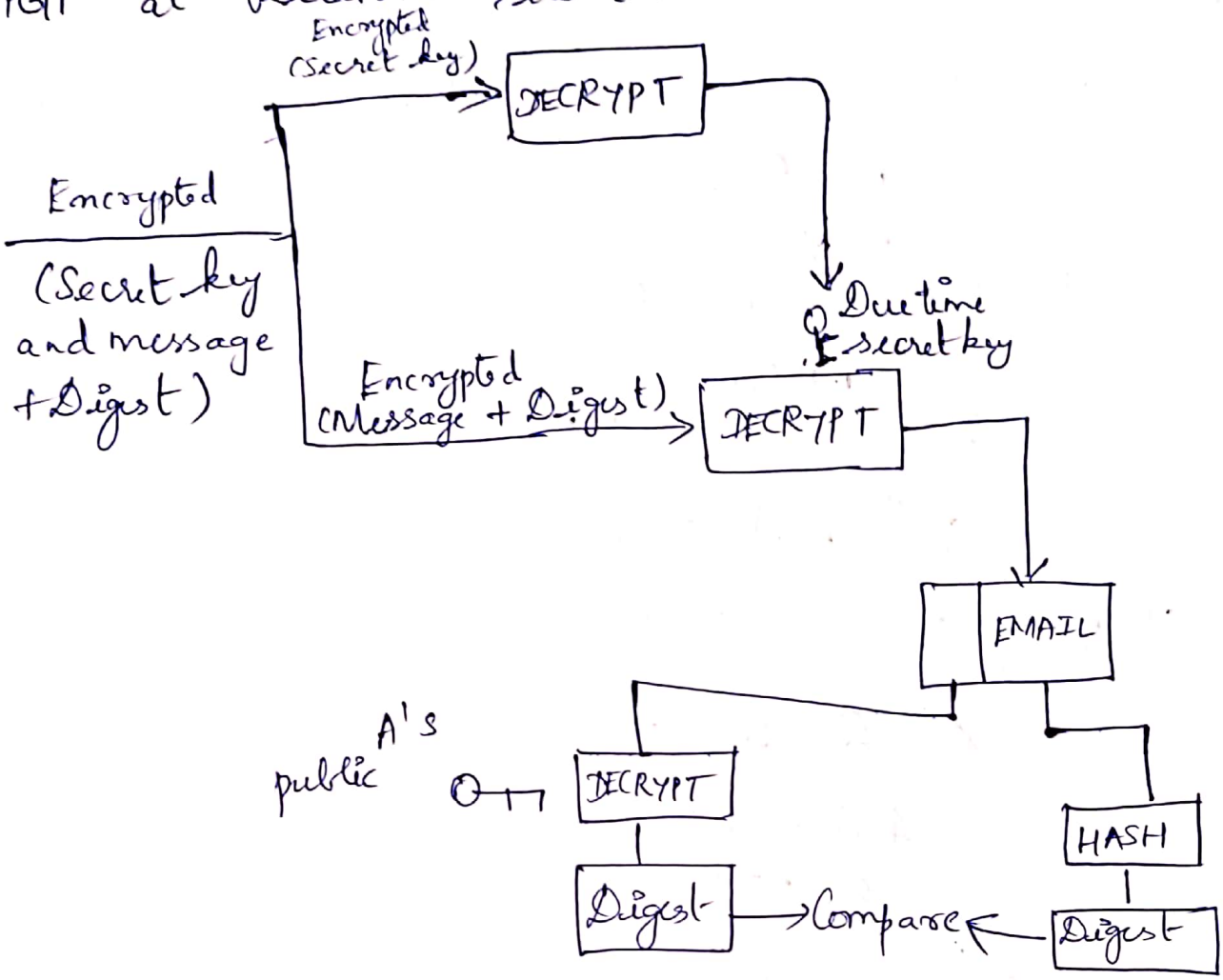
* Both the digest are compared if both of them are equal means that all the aspects of security are preserved.

PGP at Receiver site (B):

Disadvantages:

1. The administration is difficult.
2. Compatibility issues
3. Complexity
4. No recovery.

PGP at Receiver's site (B):



(12) (b) (i) DSS Scheme:-

Gn,

$q = 59$

$p = 709$

$d = 14$

$r = 13$

$e_1, e_2 = ?$

$S1, S2 = ?$

To verify the signature

$h(M) = 200$

Solution:

Primitive root of $Z_{709} = \{2, 6, 10, \ldots\}$

Choose $e_0 = 2$

$$e_1 = e_0^{(p-1)/q} \bmod p$$

$$= 2^{(709-1)/59} \bmod p$$

$$= 2^{12} \bmod 709$$

Using fast exponentiation,

- $2^2 \bmod 709$

$= 4096 \bmod 709$

$= 551$

$6 \bmod 709$

$= 36 \cdot 36 \bmod 709$

$= 46,656 \bmod 709$

$= 571$

$6^{12} \bmod 709$

$= 571 \cdot 571 \bmod 709$

$= 326041 \bmod 709$

$= 610$

$e_1 = 551$

$e_2 = e_1^{d} \bmod p$

$= 551^{14} \bmod 709$

Fast exponentiation,

$551^2 \bmod 709$

$= 303601 \bmod 709$

$= (149)^7 \bmod 709$

$149^7 \bmod 709$

$= (149)^4 (149)^3 \bmod 709$

$= (149)^{2\times 2} \cdot 55 \bmod 709$

$= (149)^{55^2} \bmod 709$

$= (149)^{3025} \bmod 709$

$= (149)^{16} \bmod 709$

$\boxed{e_2 = 259}$

$S_1 = (e_1^{r} \bmod p) \bmod q$

$= (551^{13} \bmod 709) \bmod 59$

$= (342) \bmod 59$

$= 48$

$$S_2 = (h(M) + d \times S_1) r^{-1} \bmod q$$

$$= (200 + 14 \times 48)\, 13^{-1} \bmod 59$$

$$= (200 + 672) \bmod 59 \cdot 13^{-1} \bmod 59$$

$$= (872 \bmod 59)\,(50)$$

$$= (46)(50) \bmod 59 = 2300 \bmod 59$$

$$= 58$$

VERIFICATION :

$$S_2^{-1} \bmod q$$

$$= 58^{-1} \bmod 59$$

$$= 58$$

$$V = (e_1^{h(M) \times 58}\ e_2^{48 \times 58} \bmod 709) \bmod 59$$

$$= ((551)^{200 \times 58}\ (399)^{48 \times 58} \bmod 709) \bmod 59$$

$$= (((551)^{11600} \bmod 709)\ (399^{4 \times 58} \bmod 709)) \bmod 59$$

$$= 82 \cdot 399^{2784} \bmod 709$$

$$= (82 \cdot 681 \bmod 709) \bmod 59$$

$$= (55842 \bmod 709) \bmod 59$$

$$= 579 \bmod 59$$

$$= 48$$

$S_1 = V$ Hence Verified

Part-A

①

Cryptanalytic	Non-cryptanalytic
* It is a method for circumventing the security of the cryptographic system by finding a weakness in a code, cipher or key management scheme.	→ These are the attacks which do not exploit mathematical weakness of the cryptographic algorithm but integrity, confidentiality and availability are still threatened
→ Attacking cryptosystem by looking something clever that designer didn't think of.	→ Do not use any intelligence and enumerates all possibilities
→ Eg: Plaintext analysis	Eg: Brute force attack

② $(x^3+x^2+x+1)(x^2+1)$

→ (x^4+x^3+1) as modulus

$\Rightarrow (1111)(101) = (1111) \oplus (111100)$

$= 110011$

Then,

mod 110011 with x^4+x^3+1

Left shift by 1, since degree is greater

$\Rightarrow 110011 \oplus 110010 = 1$

$((x^3+x^2+x+1)(x^2+1)) \bmod x^4+x^3+1 = 1$

③ Let us have a scenario,

Receiver's secret key is 'd' and sender's secret key is 'r'.

Sender creates 2 cipher text C_1 and C_2

$C_1 = a^r \bmod q$ (a → primitive root, q → prime num)

$C_2 \rightarrow km \bmod q$ (m → message $k = a^d \bmod q$)

C_1 is public key and C_2 is encrypted message. Since the receiver can read by the message by decrypting C_2 with C_1. Exchanging them will not allow decryption to occur, because the key is not there. It is impossible to decrypt.

④ She can't forge the message in Schnorr scheme.

In Schnorr scheme, the value of r is a one time key, which lies between $0 < r < q$.

So, she can't forge the message even if the value of r is found.

⑤ Session key:

Session key is a single used symmetric key used for encrypting all messages in one communication session

Alice —(KEY) Encryption, requests KDC for session key for communication→ Bob

It contains message, network address, Bob's network address, unique session identifier. KDC responds to A using a message encrypted key 'k'.

→ Using the master key 'k'. Alice decrypts the message, since alice and KDC only knows 'k' It is certain for alice that it is from KDC.

→ Alice keeps the session key 'ks' and sends the packet intended for Bob.

→ Bob decrypts using key 'kb'. Bob now has the session key for communication securely with Alice.

(6) Security Association:

A security association is the establishment of shared security attributes between two network entities to support secure communication.

An SA may include attributes such as cryptographic algorithm and mode, traffic encryption key and parameter for the network data to be passed over the connection.

NAME : Gowri S.
REGNUM : 2018506084

Signature S. Gowri

⑦ Formal verification and Penetration testing:

In formal verification testing, the preconditions place constraints on the state of the system when the program on system when the program on system is running.

→ In penetration testing the preconditions describe the state of the system in which the hypothesized security flaw can be exploited..

⑧ An analyst might care how similar two vulnerabilities are because they may suggest a new vulnerability with elements that are common to both of the other two vulnerabilities and they can solve them accordingly

⑨ Canonical Representation Vulnerabilities:

It can occur when a data conversion process does not convert the data to its simplest form resulting in the possible misrepresentation of the data. The app may behave in an unexpected manner when acting on input that has not been sanitized or normalised.

Eg: Only access to file under specific domain by name then all the names must be canonicalised

otherwise it will be disastrous to load files with same names

(10) Software as an Intellectual property.

Software can be protected as an intellectual property by the following measures.

- → Patents
- → Copyright
- → Trade Secrets
- → Trade marks

→ A Software license is also a good method to protect a software

PART-B

(12)

(b)

(ii) → Elgamal Encryption is an public key cryptosystem.

→ Uses Asymmetric key for communication

IDAA:

Suppose Alice wants to communicate to Bob.

(i) Bob generates public and private key.

Bob chooses a very large number q and cyclic group F_q.

An element a such that $gcd(a, q) = 1$

Then, he computes $h = g^a$

F, $h = g^q$, q and g as his public key

(2) Alice encrypts

Selects element k from F such that $gcd(k, q) = 1$

Computes $p = g^k$ and $s = h^k = g^{ak}$

She multiplies with M

Sends $(p, M * s) = (g^k, M * s)$

(3) Decryption

Calculates $s' = p^a = g^{ak}$

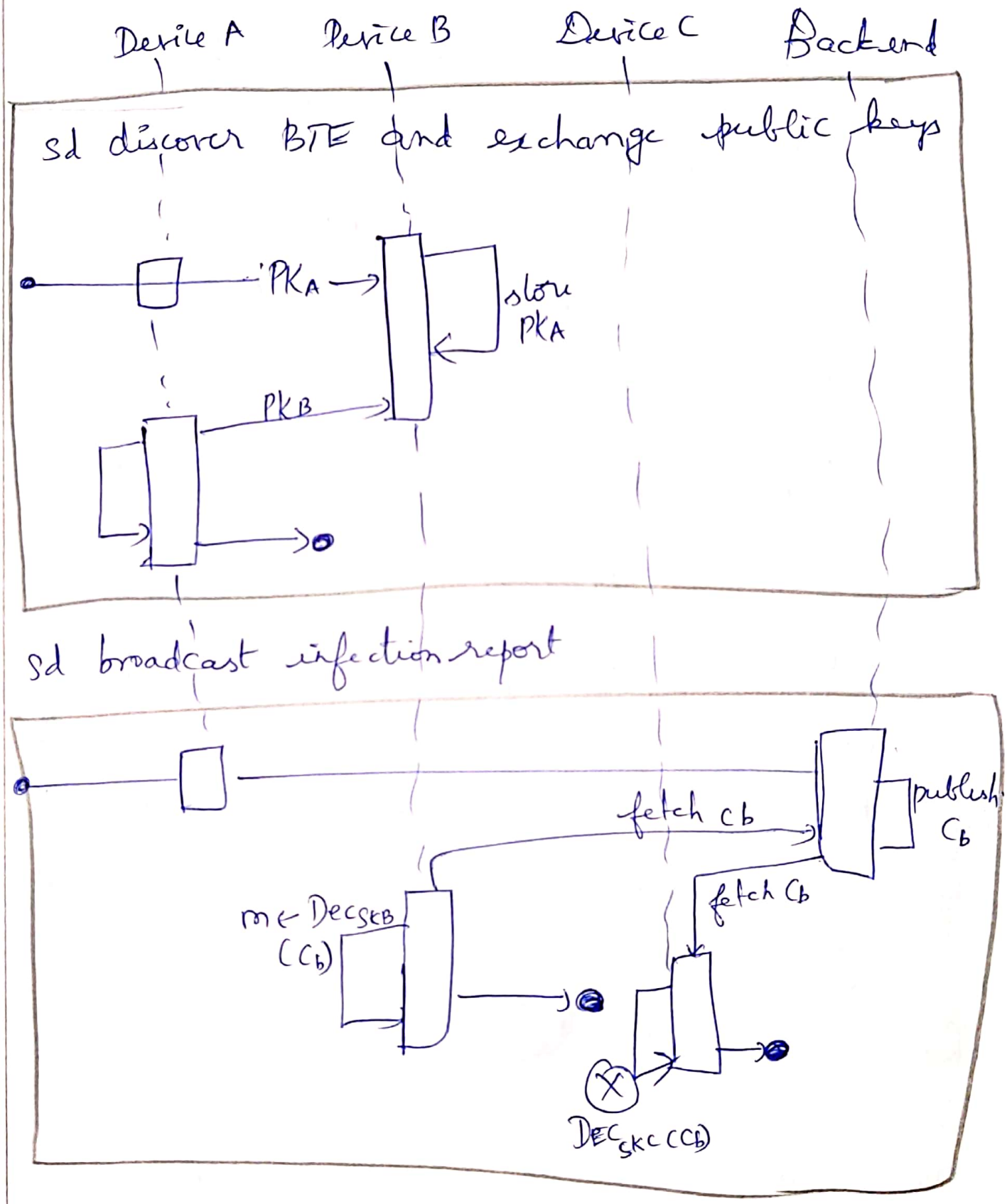
Divides $M * s$ by s' to obtain M as $s = s'$

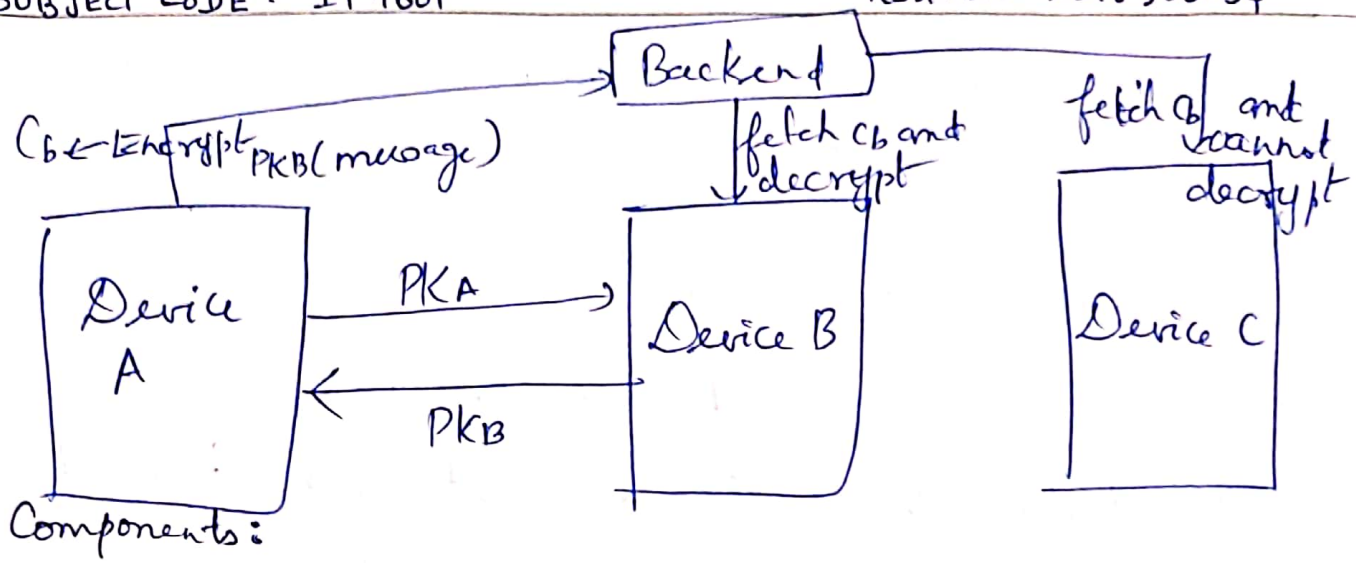
PART - C

(16) For the protection of people and society against harm and health threats, especially for the COVID-19 pandemic, a variety of different disciplie needs to be followed.

Data Collection is very basic and health related data of individuals in today's mobile society does to help to plan protect and identify next step health authorities

and the goverments can, shall or need to plan for or even implement.





Components:

Device:

The device is assumed to be trusted because secret keys must remain private and thus data generated and broadcasted is trustworthy.

Backend:

Backend is assumed not to be trusted concerning confidentiality, integrity and availability. Therefore devices are required to encrypt any message, including notification messages, with the public key of devices that had been received in close proximity over a difficult period time. Therfore, a interaction scheme is applied where public keys are exchanged

regularly while devices are near and reachable via BLE

Communication Channel..

It is provided by the BLE advertisements which are not to be trusted. Thus a service provider cannot assure the availability of the service (ie) messages can fail to be delivered and their content is readable from anyone receiving the message if not an explicitly encrypted payload is maintained..

Revealing identity of the device running this communications may be possible with external meta-data from service provider.

• All the answers in this answer booklet have been written in my own handwriting. Nobody has helped me in writing the answers.