Assignment No.-02

Q.1. Explain in detail about Eulers Totient function?

Ans:- Eulers totient function is the mathematical multiplicative function that counts the positive integers up to the given integer generally callend 'n' which is a prime number to 'n'.

One may use the function to know the number of prime number that exist up to the given integer n.

It is denoted as '$\phi(n)$'.

Properties of Eulers Totient function.

1) ϕ is the symbol used to denote the function and deals with a prime number
2) The function is applicable only in the case of positive integers.
3) If integers 'n' is a prime number then gcd (m, n) = 1
4) In genral equation is

$$\phi(mn) = \phi(m) * \phi(n)(1 - 1/m)(1 - 1/n)$$

4) If the given number p is prime then $\phi(p) = p-1$

5) $\phi(10^n) = 4 * 10^{n-1}$

Calculation of Euler's Totient function :-

Example :- Calculate $\phi(7)$?

$\phi(7) = (1, 2, 3, 4, 5, 6) = 6$

Example 2 :- Calculate $\phi(100)$?

$$\phi(100) = \phi(m) * \phi(n)\,(1-1/m)\,(1-1/n)$$

$$= \phi(100) = 2^2 * 2^5$$

$$= \phi(100) = 2^2 * 2^5 * (1-1/2)\,(1-1/5)$$

$$= 100 * 1/2 * 1/5$$

$$= 40$$

Q.2) In public key system using RSA you intercept the cipher text C = 10 sent to the user whose public key is e = 5, n = 35, what is plaintext M ?

Ans:- Given :-

cipher text C = 10

e = 5

n = 35 = 7 x 5

The value of p and q must be prime, we consider that

p = 7, q = 5

Step 1 :- Calculate $\phi(n)$

$= (p-1)(q-1)$

$= (7-1)(5-1)$

$= 6 \times 4$

$= 24$

Step 2 :-

$e * d \bmod \phi(n) = 1$

$5 * d \bmod 24 = 1$

$5 \times d \div 24 = i + 1$

$d = \frac{24 * i + 1}{5}$ if $i = 1$

$= \frac{24 * 1 + 1}{5} = \frac{24+1}{5} = \frac{25}{5} = 5$

$\boxed{d = 5}$

Step 3 :-

$$P = e^d \bmod n$$

$$= 10^5 \bmod 35$$

$$\boxed{P = 5}$$

∴ The plaintext M is = 5

Q.2 b) Demonstrate the working of Define Hellman key exchange algorithm with suitable example.

Ans:- The define Hellman key exchange algorithm allows two parties to securely exchange a shared secret key over an insecure communication channel.

~~Working~~ :-

~~1. Key generation~~ :-

Working :-

1. Installation :- Lets say Aman and Bhushan wants to establish a shared Secrete key.

2. Aman and Bhushan choose their own private key and calculate their public key using the value of P, g.

Calculate $A = (g^a) \bmod p$.

Calculate $B = (g^B) \bmod p$

3. Exchang publick keys between Aman and bhushan and Compute the Shared Secrete key by using the formula as :-

Aman Compute the Shared Secrete key S. as $S = (B^a) \bmod p$.

Similarly, ~~For~~ Bhushan compute.

$S = (A^p) \bmod p$.

After that both arrived Same Secrete key.

Example:-

1. Aman and Bhushan on;
   - Prime number $p = 25$
   - Primitive root $g = 6$

2. Aman choose a private key $a = 4$ and calculate public key
   $A = (6^4) \bmod 25 = 21$

3. Both chooses a private key $b = 10$ and calculate his public key
   $B = (6^{10}) \bmod 25 = 1$

4. Aman sends A(21) to Bhushan and Bhushan sends B(1) to Aman.

5. Aman Compute Shared secrete key:
   $S = (1^4) \bmod 25 = 1$

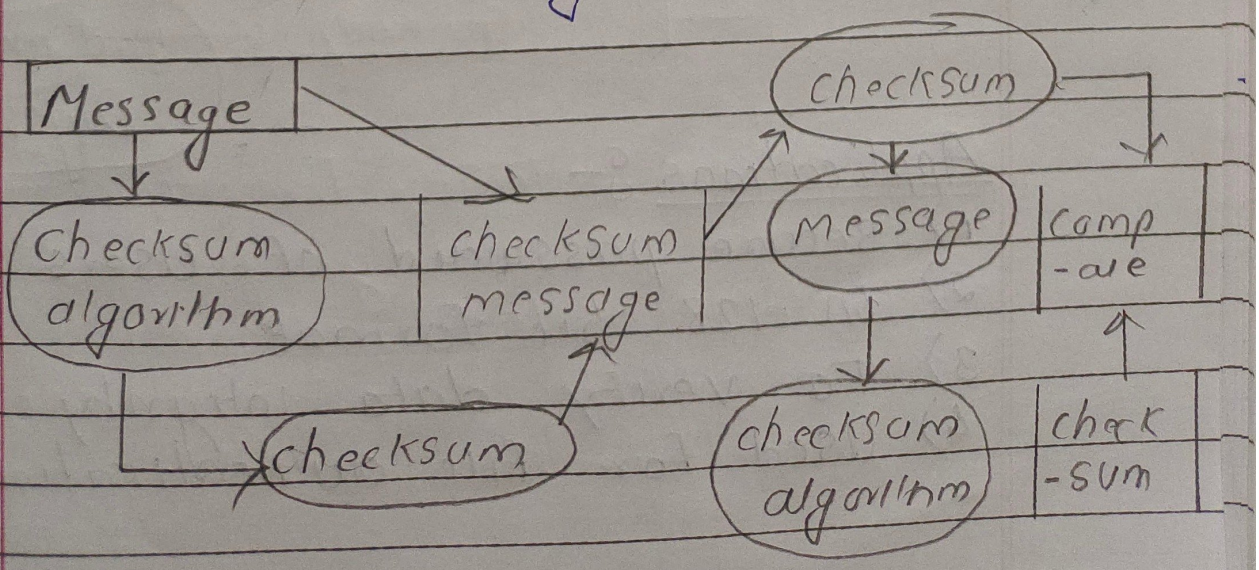
6. Bhushan compute Shared Secrete key:
   $S = (21^{10}) \bmod 25 = 1$

Now, Aman and Bhushan have the same shared secrete key, Hence they can use for secure Communication.

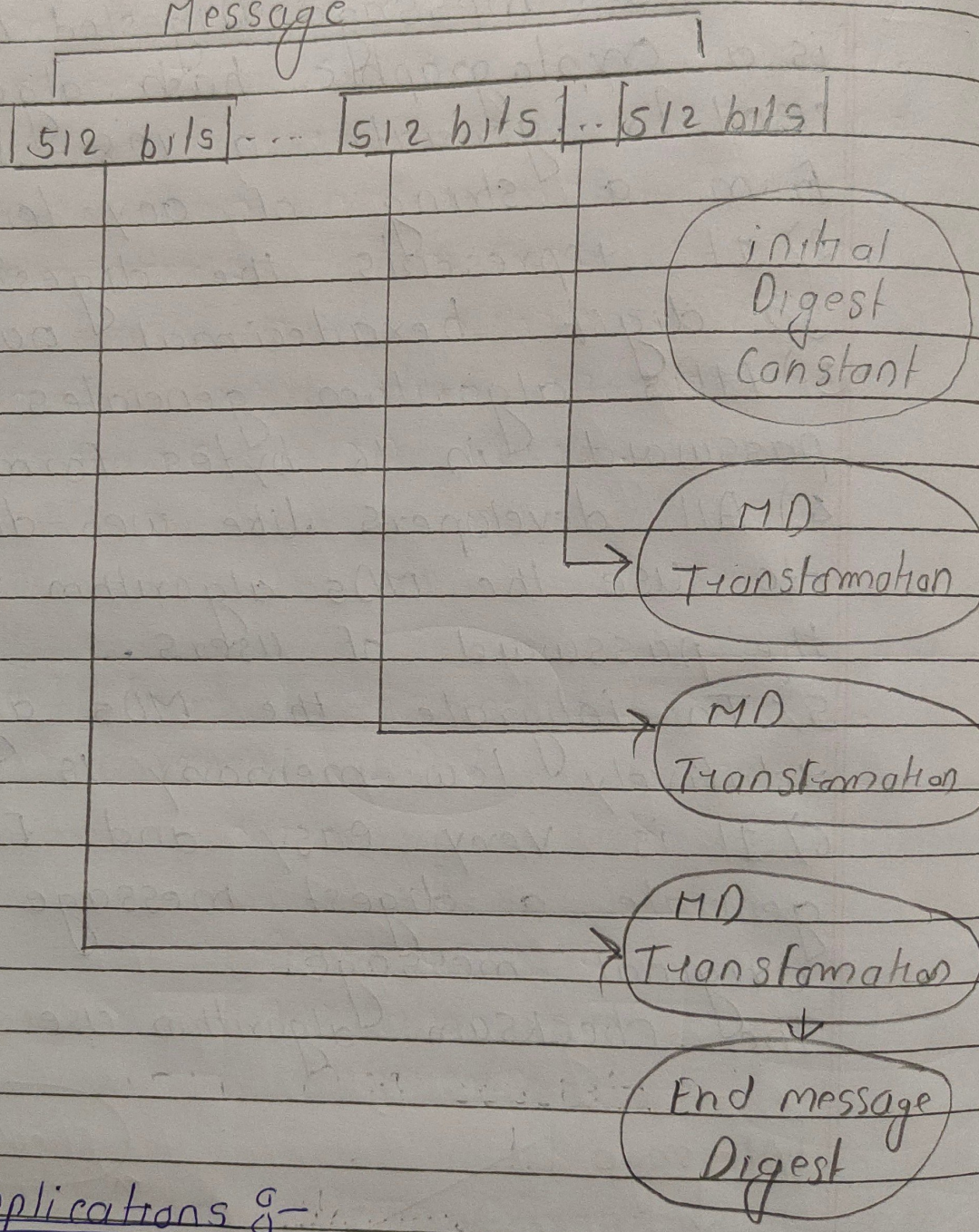
Q.3 Explain in detail about MD5 Message Digest Algorithm.

Ans:-

1) MD5 (message Digested Algorithm is a cryptographic hash algorithm used to generate a 128-bit digest from a string of any length.
2) It represents the digested as 32 digit hexadecimal numbers.
3) MD5 algorithm generates a strong password in 16 bytes format.
4) All developers like web developers etc use the MD5 algorithm to secure the password of users.
5) To integrate the MD5 algorithm, relatively low memory is necessary
6) It is very easy and faster to generate a digest message of the original message.
The checksum algorithm use in MD5.



The MD5 operates on message 512 bits at a time



Applications :-

1) Secure password of users
2) In 128 bit format
3) To verify data integrity
4) Used for file authentication.

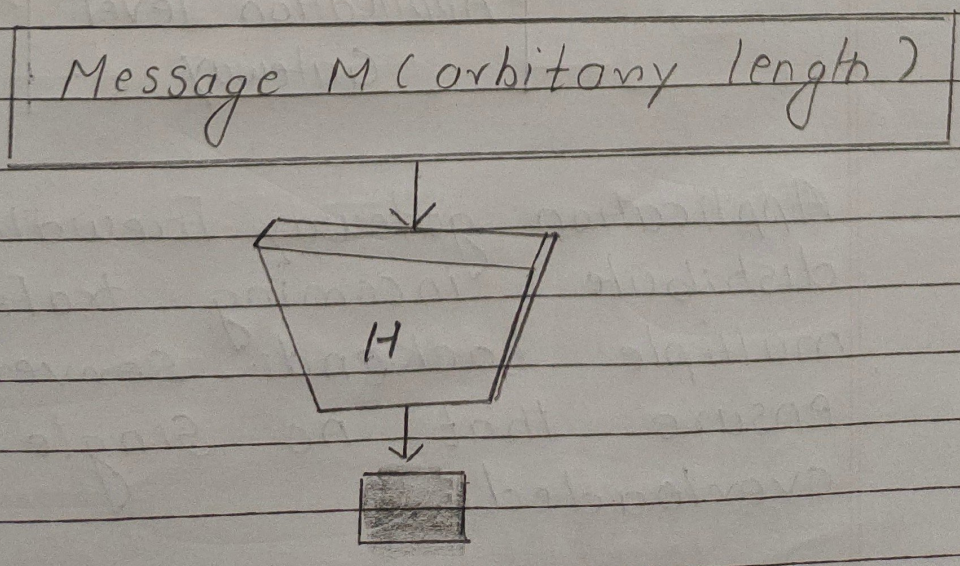
Q.4 Explain the Hash functions and their security.

Ans:- 1) Hash functions are commonly used data structures in computing systems for tasks such as checking the integrity of message and authenticating information.

2) While they are considered crypto-graphically "weak" because they can be solved in polynomial time, they are not easily decipherable

3) Hash functions are extremely useful and appear in almost all information security applications.

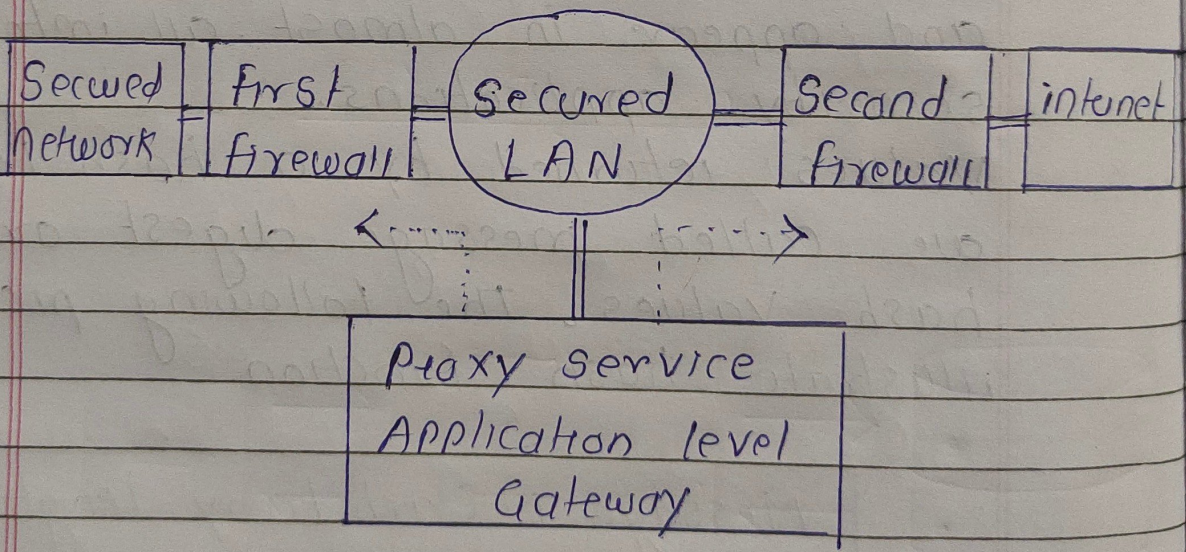
Values returned by a hash function are called message digest or simply hash values. The following picture illustrate hash function.



Q.5 Explain in detail about Application Gateway firewall.

Ans:- 1) Application gateway firewall opeidte at the application layer (layer 7) of the OSI model.

2) They filter access based on application definitions. Application ~~determitions~~ definitions can include not only port numbers but also specific application information like acceptable HTTP verbs.



Application gateway firewall can distribute incoming trafic across multiple backend servers to ensure that no single one is overloaded.

Benifits of using an application level gateway Firewall :-

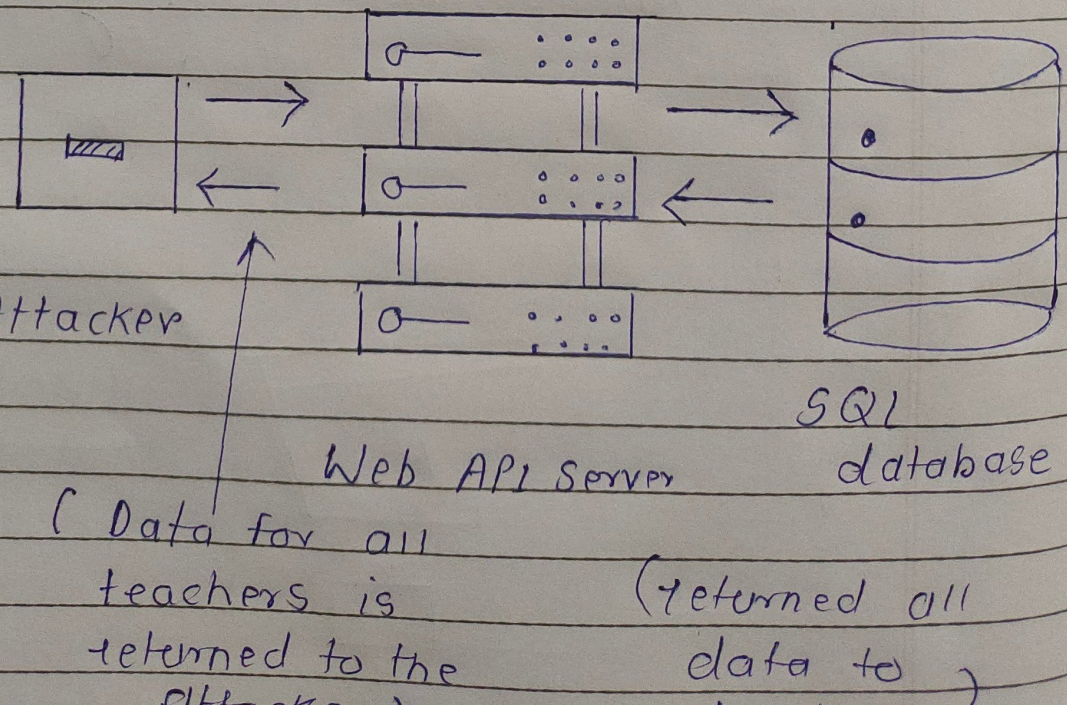
1. Increase Security
2. Allows traffic logging
3. Support Content caching
4. Network performance improvement
5. layered access model.

Q.6 Explain detail about SQL injection?

Ans:- 1) SQL injection, also known as SQLI is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed.

2) This information ~~any~~ may include any number of items, including sensitive company data, user lists or private customer details.

SQL Injection



Type of SQL Injection :-

1. In-band SQLi

• Error based SQLi - The attacker performs actions that cause the database produce error message

2. Inferential (Blind) SQLi :-

This method is called blind SQLi because the data is not transfered from the website database to the attacker.

3. Out-of-band SQLi

Out of band SQLi is performed when the attacker can't use the same channel to launch the attack and gather information.

SQL injection example :-

Can be altered to read http://www.estore.com/items/items.asp?itemid=999 or 1=1

As a result, SQL query look like this :-

```
SELECT ItemName,
ItemDescription
FROM Items
WHERE ItenNumber = 999 OR
1=1
```