**INFORMATION SECURITY QUESTION BANK**

**INFORMATION SECURITY**

1. What is information security? And types of security.
2. What is vulnerability, risk, threat and exploit?
3. Why do we need security in Information System?
4. What are the components of Information System?
5. Describe any ten categories of threats.
6. Describe any ten categories of software attacks.
7. What is linear block code, code rate, hamming distance and hamming weight?
8. What are the critical characterstics of Information?
9. What is social engineering and phishing?
10. What is sabotage, information extortion and espionage?
11. Explain Security System Development Lifecycle (SDLC) & Security SDLC.
12. What is an intrusion detection prevention system (IDPS)?
13. What are honey pots and honey net?
14. Name some scanning and analysis tools.
15. For a (8, 4) code, Parity Matrix is given:

P = 1 1 1 0 a) Find the Generator and Parity Check Matrix.

1 1 0 1

0 1 1 1 b) Find out all possible codewords.

1 0 1 1

c) Find minimum weight of this code.

**CRYPTOGRAPHY**

1. What is cryptography and cryptanalysis?
2. What are substitution ciphers? Give some examples.
3. What is additive, multiplicative and affine cipher?
4. What is vigenere cipher and hill cipher?
5. Explain the working of rotor cipher and enigma cipher.
6. What are transposition ciphers?
7. What is d-box and its types?
8. What is s-box?
9. What is a digital signature? And mention its services.
10. Explain rabin cryptosystem.
11. How is email security implemented?

**SOLUTIONS**

**INFORMATION SECURITY**

1. Information security is to protect the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission. It is achieved via the application of policy, education, training and awareness, and technology.

A successful organization should have the following multiple layers of security in place to protect its operations:

* **Physical security**, to protect physical items, objects, or areas from unauthorized access and misuse
* **Personnel security**, to protect the individual or group of individuals who are authorized to access the organization and its operations
* **Operations security**, to protect the details of a particular operation or series of

activities

* **Communications security**, to protect communications media, technology, and content
* **Network security**, to protect networking components, connections, and contents
* **Information security**, to protect the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission. It is achieved via the application of policy, education, training and awareness, and technology.

1. **Vulnerability:** A weaknesses or fault in a system or protection mechanism that opens it to attack or damage. Some examples of vulnerabilities are a flaw in a software package, an unprotected system port, and an unlocked door.

**Risk**: The probability that something unwanted will happen. Organizations must minimize risk to match their risk appetite—the quantity and nature of risk the organization is willing to accept.

**Threat**: A category of objects, persons, or other entities that presents a danger to an

asset. Threats are always present and can be purposeful or undirected. For example,

hackers purposefully threaten unprotected information systems, while severe storms

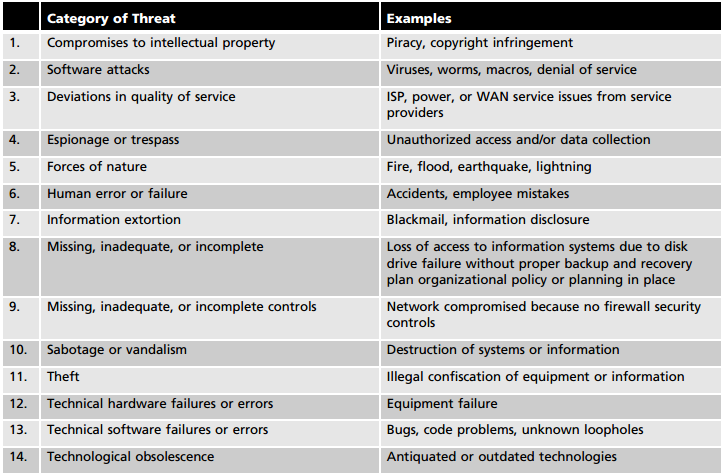
incidentally threaten buildings and their contents.

**Exploit:** A technique used to compromise a system. This term can be a verb or a noun. Threat agents may attempt to exploit a system or other information asset by using it illegally for their personal gain. Or, an exploit can be a documented process to take advantage of a vulnerability or exposure, usually in software, that is either inherent in the software or is created by the attacker.

1. Information security is required to performs these important functions for an organization:

* 1. Protecting the organization’s ability to function
* 2. Enabling the safe operation of applications running on the organization’s IT systems
* 3. Protecting the data the organization collects and uses
* 4. Safeguarding the organization’s technology assets

1. Components of Information security are : Software , Hardware, Network ,Data, People, Procedures.
2. **THREATS**



1. **SOFTWARE ATTACKS:**

* Malicious code
* Hoaxes
* Back Doors
* Password Crack
* Brute Force
* Dictionary
* Denial of Service
* Spoofing
* Man in the middle
* Spam
* Mail bombing
* Sniffers
* Social Engineering
* Phishing
* Timing Attack

1. **Linear Block code :**  is a set of linear codewords of length n and message size k. A linear code is an error-correcting code for which any linear combination of codewords is also a codeword.

**Code rate:** It is the ratio of message and length of code ( k/n)

**Hamming Distance:** It is the number of bits that differ in any two codewords.

**Hamming Weight:** It is the number of on zero components in a codeword.

1. Critical Characterstics of Information Security :

* Availability
* Accuracy
* Authenticity
* Confidentiality
* Integrity
* Utility
* Possession

1. **Social Engineering** : n the context of information security,social engineeringis the process of using social skills to convince people to reveal access credentials or other valuable information to the attacker. There are several social engineering techniques, which usually involve a perpetrator posing as a person higher in the organizational hierarchy than the victim.

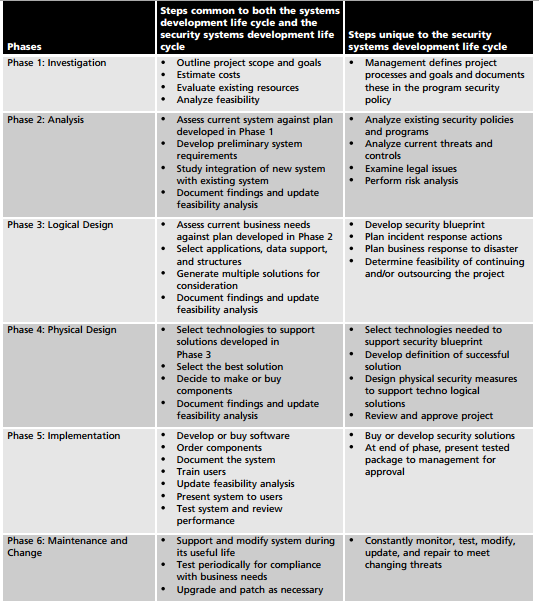
**Phishing** is an attempt to gain personal or financial information from an individual, usually by posing as a legitimate entity. Phishing attacks use three primary techniques, often in combination with one another: URL manipulation, Web site forgery, and phone phishing.

1. **Sabotage** : This category of threat involves the deliberate sabotage of a computer system or business, or acts of vandalism to either destroy an asset or damage the image of an organization. These acts can range from petty vandalism by employees to organized sabotage against an organization.

**Information Extortion**: Information extortion occurs when an attacker or trusted insider steals information from a computer system and demands compensation for its return or for an agreement not to disclose it.

**Espionage:** Espionage or trespass is a well-known and broad category of electronic and human activities that can breach the confidentiality of information. When an unauthorized individual gains access to the information an organization is trying to protect, that act is categorized as espionage or trespass.

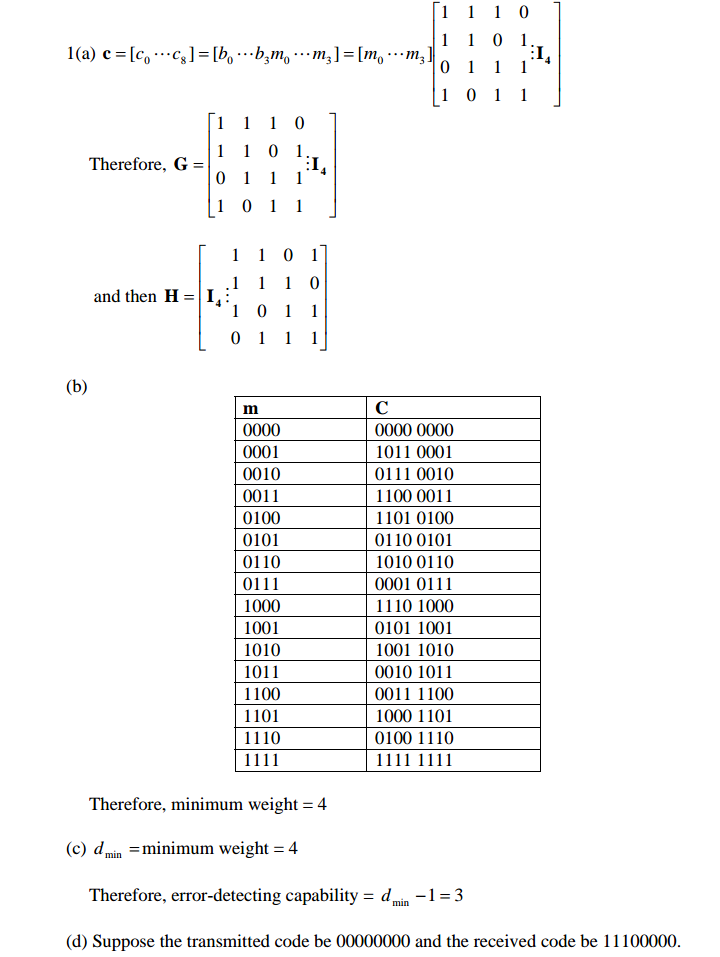
1. **System Development Lifecycle (SDLC) & Security SDLC**



1. An Intrusion **Detection and Prevention System (IDPS)** is a network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits. Vulnerability exploits usually come in the form of malicious inputs to a target application or service that attackers use to interrupt and gain control of an application or machine.
2. **Honey pot** are decoy systems designed to lure potential attackers away from critical systems. In the industry, they are also known as decoys, lures, and fly-traps. When a collection of honey pots connects several honey pot systems on a subnet, it may be called a **Honey net**.
3. **Scanning Analysis Tools :**

* Port Scanners
* Firweall Analysis Tools
* Operating System Detection Tools
* Vulnerability Scanners
* Packet Sniffers
* Wireless Security Tools

1. G = [P : I ] H = [I : P’]



**CRYPTOGRAPHY**

1. **Cryptography**: Science and art of transforming messages to make them secure and immune to attacks. It is secret writing. In a broader sense: Mathematical techniques related to information security. It is about secure communication in the presence of adversaries.**Cryptanalysis**: Science and art of breaking codes. It helps us to create better codes.
2. Substitution cipher replaces one symbol with another. Examples: Additive, Multiplicative,Affine ,Vigenere ,Hill ,One Time Pad, Rotor Cipher, Enigma Machine.
3. **Additive**: It is a substitution **cipher** where each letter in the original message (called the plaintext) is replaced with a letter corresponding to a certain number of letters up or down in the alphabet. Encryption: C(i) = [x +P(i)]mod 26 Decryption: P(i) = [x +C(i)]mod 26

**Multiplicative**: Encryption algorithm specifies multiplication of plaintext by the key and decryption algorithm specifies division of cipher text with key.

Encryption : C(i) = [m . p(i)]mod 26 Decryption : P(i) = [m-1 . C(i)]mod 26

These are the 12 positive integers that are less than 26 and relatively prime to 26. So, there are only 12 possible multiplicative keys, and one of them is 1 which would make the cipher text alphabet the same as the plaintext alphabet.

**Affine cipher**: is a type of wherein each letter in an alphabet is monoalphabetic substitution cipher, mapped to its numeric equivalent, encrypted using a simple mathematical function, and converted back to a letter.

Encryption: C(i) = [a. p(i) +b]mod 26 Decryption C(i) = a-1 .[ p(i) -b]mod 26

a: multiplicative key and b: additive key

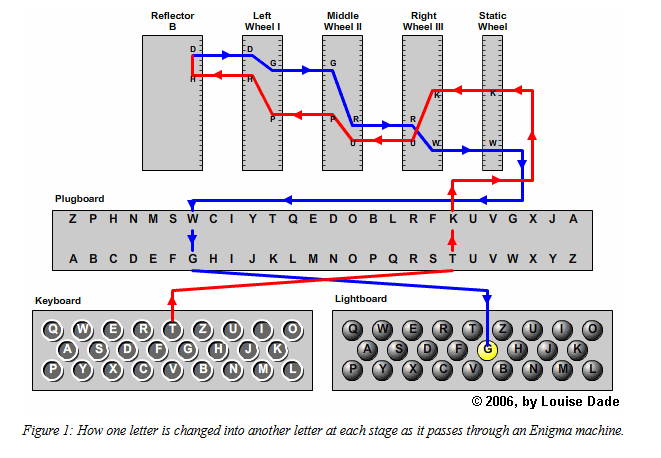
1. **Vigenère** cipher is a method of encrypting alphabetic text by using a series of different Caesar ciphers based on the letters of a keyword. It is a simple form of polyalphabetic substitution. This scheme of cipher uses a text string (say, a word) as a key, which is then used for doing a number of shifts on the plaintext. Each plaintext character has been shifted by a different amount and that amount is determined by the key.

**Hill Cipher** is a polyalphabetic cipher based on linear algebra. Hill used matrices and matrix multiplication to mix up the plaintext. They are block ciphers.Plaintext is divided into equal size blocks. The blocks are encrypted one at a time in such a way that each character in the block contributes to the encryption of other characters in the block. Key is a square matrix of size m x m , mi is size of the block. To get our cipher text we perform a matrix multiplication.

1. **Rotor cipher** : Each rotor maps 26 characters on the front face to 26 on the back face

Simple substitution cipher .After each encoding rotation changes the mapping Introduces polyalphabetic element with period 26 .The output of one rotor feeds the next .The key is the rotor wiring, placement, and initial position.

**Enigma Machine**: It is based on rotors. It uses 3 rotors, 1 reflector, keyboard, plug board and lamp board. The Enigma machine is an electro-mechanical device. It is mechanically operated, with an electric signal passed through wires and various mechanical parts. The easiest way to explain the mechanics is to follow the journey of a single letter from keyboard to lamp board.



Example:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **III** | **II** | **I** | **Reflector** | **Inv I** | **Inv II** | **Inv III** |
| G->C | C->D | D->F | F->S | S->S | S->E | E->P |
| A->B | B->J | J->Z | Z->T | T->L | L->K | K->U |

Rotor III ABCDEFGHIJKLMNOPQRSTUVWXYZ  
 BDFHJLCPRTXVZNYEIWGAKMUSQO

Rotor II ABCDEFGHIJKLMNOPQRSTUVWXYZ  
 AJDKSIRUXBLHWTMCQGZNPYFVOE

Rotor I ABCDEFGHIJKLMNOPQRSTUVWXYZ  
 EKMFLGDQVZNTOWYHXUSPAIBRCJ

Reflector B ABCDEFGHIJKLMNOPQRSTUVWXYZ  
 YRUHQ S LDPXNGOKMIEBFZCWVJAT

1. Transposition cipher is asimple data encryption scheme in which plaintext characters are shifted in some regular pattern to form cipher text. It does not substitute one symbol for another, instead it changes the location of the symbols. It REORDES symbols.
2. D-box is diffusion box. It parallels transposition cipher for characters. It transpose bits

Types: Straight D-box (no of inputs=no of outputs)

Expansion D-box (no of inputs < no of outputs)

Compression D-box (no of inputs > no of outputs)

1. In cryptography, an **S-box** (**substitution-box**) is a basic component of symmetric key algorithms which performs substitution. In block ciphers, they are typically used to obscure the relationship between the key and the cipher text — Shannon's property of confusion. In general, an S-box takes some number of input bits, *m*, and transforms them into some number of output bits, *n*, where *n* is not necessarily equal to *m*. A *m*×*n* S-box can be implemented as a lookup table with 2*m* words of *n* bits each.
2. **Digital Signature** is a digital code (generated and authenticated by public key encryption) which is attached to an electronically transmitted document to verify its contents and the sender's identity. A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or documents. Services: Message authentication, message integrity, non repudiation by third party, confidentiality by cryptography.
3. **Rabin cryptosystem** , devised by M.Rabin , is a variation of the RSA cryptosystem.

* RSA : C ≡ Pe (mod n) P ≡ C ^d (mod n)
* It can be thought be of RSA with fixed values e=2 d=1/2
* n= p \* q ; p and q are prime numbers in the form 4k+3, p≠q
* Public Key : n
* Private Key : (n,q)
* Asymmetric Key system.

Encryption

* C=P^2 (mod n)

Decryption

* a1 = +(C ^((p+1)/4))mod p
* a2 = -(C ^((p+1)/4))mod p
* b1 = +(C ^((q+1)/4))mod q
* b2 = -(C ^((q+1)/4))mod q
* P1= Chinese\_Remainder (a1,b1,p,q)
* P2= Chinese\_Remainder (a1,b2,p,q)
* P3= Chinese\_Remainder (a2,b1,p,q)
* P4= Chinese\_Remainder (a2,b2,p,q)
* Four equally probable plaintext : P1,P2,P3,P4 .

EXAMPLE :

* p=23 q=7 both in 4k+3 form
* n=p\*q=161
* Public key n is announced , p and q kept private.

Plaintext=24 C=P^2 mod n (ENCRYPTION)

* C=24^2mod 161= 93 93 is Cipher text

Now calculate Plaintext ( DECRYPTION)

* a1= + (93^(23+1)/4) mod 23 = 1
* a2= - (93^(23+1)/4) mod 7 = 22
* b1= + (93^(7+1)/4) mod 7 = 4
* b2= - (93^(7+1)/4) mod 7 = 3

By 4 taking possible ans (a1,b1) (a1,b2) (a2,b1) (a2,b2) & using chinese remainder theorem we get 4 possible plaintext : 116, 24 , 137,45.

1. **Email** is a one time activity. In Email there is a unidirectional message between the sender and receiver. Since there is no session or handshaking, the sender of the message needs to include name or identifiers of the algorithms used in the message. Encryption/Decryption is done using a symmetric-key algorithm, but the secret key to decrypt the message is encrypted with the public key of the receiver and is sent with the message.