**UNIT DCS01 CRYPTOGRAPHY**

**Task 1**

**1.Define the concept and application of cryptography**

Cryptography relates to the process of converting plain text into unintelligible text and vice-versa, it is used to encrypt data and decrypt data. Cryptography is also a method of storing and sending data in a particular unreadable form so that only those for whom it is intended to can read and process it. Cryptography does not only protect the data from theft or alteration but can also be to authenticate users.

**2.Explain symmetric and asymmetric modes and approaches.**

**Symmetric**

Symmetric encryption is one of the most popular and widely used data encryption method, using this method data is encrypted and decrypted using a single secret cryptographic key. It is used daily in many major industries, including defense, banking, health care, and other industries where sensitive data is very important.

**The Popular examples of symmetric encryption include the:**

**\* Advanced Encryption Standard (AES)**

AES encryption is a method which uses block ciphers of 128, 192, or 256 bits to encrypt and decrypt data, is one of the most well-known and effective symmetric encryption methods used today. It would take billions of years to crack, and that’s why it’s used to secure sensitive, secret, or classified information in government, healthcare, banking, and other industries. It is more secure than DES, Triple DES, and IDEA.

**\* TLS/SSL protocol**

Using this method, a unique key, called session key, is generated, whenever a client accesses a server, These session keys are used to encrypt and decrypt the data sent between the client and the server in that specific client-server session at that specific point in time.

**One of the advantages of symmetric encryption include:**

Symmetric encryption algorithms like AES take billions of years to crack using brute-force attacks also because of its shorter key lengths and relative simplicity compared to asymmetric encryption, is much faster to execute.

**Disadvantages of symmetric encryption include:**

If this secret key is stored in an insecure location on a computer, then hackers could gain access to it using software-based attacks, allowing them to decrypt the encrypted data and thereby defeating the entire purpose of symmetric encryption. For scalability a different key is required for each communication between people and has limited functionality whereas symmetric systems can't provide authentication.

**Asymmetric encryption**

Asymmetric encryption, also known as public-key cryptography or public-key encryption, uses mathematically linked public- and private-key pairs to encrypt and decrypt senders’ and recipients’ sensitive data. Asymmetric encryption uses different keys to encrypt data and decrypt data.

**Examples of asymmetric encryption include:**

**\*Rivest Shamir Adleman (RSA)**

RSA is one of the oldest examples of asymmetric encryption. RSA encryption generates a public key by multiplying two large, random prime numbers together and using these same prime numbers, generates a private key, then data is encrypted using the public key and decrypted using the private key, same way as

**\*Elliptical Curve Cryptography (ECC)**

ECC is an RSA alternative that uses smaller key sizes and mathematical elliptic curves to execute asymmetric encryption. It’s frequently used to digitally sign cryptocurrency transactions. ECC is much faster than RSA in terms of key and signature generation.

**\*TLS/SSL protocol**

TLS/SSL uses asymmetric encryption to establish a secure client-server session while the client and server are generating symmetric encryption keys, this process known as a TLS handshake. After the TLS handshake is complete, the client-server session keys are used to encrypt the information exchanged in that session.

**One the advantages of using asymmetric encryption include:**

Asymmetric encryption eliminates key distribution entirely. The needed public keys are exchanged through public-key servers, and the disclosure of public keys is not, at this time, detrimental to the security of encrypted messages, because they cannot be used to derive private keys, with asymmetric encryption, senders can use their private keys to digitally sign and verify data originated from them.

**One the disadvantages of using asymmetric encryption include:**

Asymmetric encryption is that it’s slower than symmetric encryption because of its longer key lengths, not to mention that asymmetric encryption calculations tend to be much more complex than their symmetric counterparts.

**3. Assess how cryptographic methods and standards underpin the communications security of cyber-enabled networks and devices**

Cryptographic methods are used to protect data in the network from unauthorized access and various threats. These methods offer security, which enhances the usability and integrity of the network. The design aspects of the network security mechanism involve both hardware and software technologies. The application domains of security mechanisms cover both public and private computer networks which are used in everyday jobs for conducting transactions and communications among business partners and individuals. The network security schemes vary depending on the types of the network, that is, public or private, wired or wireless. Data security includes encryption, tokenization, and key management practices in protecting data across all applications and platforms. The antivirus and antimalware softwares are also part of network security for protection from malware such as spyware, viruses and other threats. Cryptography is an automated mathematical tool that plays a vital role in network security. It assures the confidentiality and integrity of data as well as provides authentication and non-repudiation to the users. Cryptography methods consists of encryption and decryption algorithms.

The cryptographic algorithms that are widely accepted are outlined with their relative advantages and disadvantages. Moreover, recent proficient cryptographic algorithms specific to cloud computing, wireless sensor networks and on-chip-networks are thoroughly discussed that provide a clear view about acquiring secure communication in the network using cryptography.

**Task 2**

**2.1: Explain the key principles of the related standards, regulations and laws and why they are in place.**

Encryption is relied on to protect the data and computer systems of individuals and organizations from criminals and repressive governments. The public's use of encryption can prevent crimes such as business attacks which occur when there is lack of expertise.

Companies that transmits, processes or stores card payment details are required to submit an annual self-assessment and network scan by the PCI DSS, or to complete an onsite PCI data security assessments and quarterly network scans as well as to do the following:

**1. Build and maintain a secure network:**

A business must install and maintain a firewall configuration to protect credit card data, must not use vendor-supplied defaults for system passwords and other security parameters.

**2. Protect cardholder data:**

Encrypt transmission of cardholder data across open or public networks.

**3. Maintain a vulnerability management program:**

A business but use and regularly update the antivirus software as well as develop and maintain secure systems and applications

**4. Implement strong access control measures:**

A business must restrict access to cardholder's data from unknown people and must assign a unique identifier to each person who has access to the computer as well as restrict physical access to cardholder's data.

**5. Regularly monitor and test networks:**

Monitor and track all access to the network's resources and cardholder details. Regularly test security systems and processes.

**6. Maintain an information security policy:**

A business must maintain its policy that addresses information security such as the acceptable use of the organization's information, including networks and applications to protect data confidentiality, integrity, and availability.

An organizational structure must understand where their business is being conducted. Know what rules apply to your organization, particularly when you have international locations. Know what you need to encrypt. Any sensitive data types that need to be protected for regulatory compliance or to comply with internal policies and standards can be strong candidates for encryption. If you have a data classification policy, encrypt the most sensitive or critical category (or the top two most sensitive categories). Understand data formats such as [4digits].

Data protection laws are enacted to protect information collected and maintained on individuals from unauthorized disclosure or misuse. Privacy laws are one area in which the United States lags behind many others, particularly, regulations that prohibit the transfer of personal information to countries (including the United States) that does not protect such information. The EU privacy rules include requirements about personal data collection such as data must be collected fairly and lawfully, must only be used for purposes it was collected for, must be accessible to individuals who request a report on personal information held about them, transmission of personal data to locations where equivalent privacy protection cannot be assured is prohibited, personal data can't be disclosed to other organizations or individuals and must be accurate and kept up to date.

**2.2: Assess the consequences for organizations and individuals of non-compliance with these standards, regulations and laws.**

Organizations and individuals who are non-compliance the standards, regulations and laws will be fined by the Information Commissioner's Office. If a business processes or stores card payment details. Compliance is mandated and enforced by payment card brands such as MasterCard and Visa, these business are required to build and maintain a sure network, protect the cardholder's data and encrypt transmission of cardholder data across public networks, If these requirements are not met, penalties for non-compliance business, are levied by the payment card brands, the business will not be able to process credit card transactions and will be fined up to $25,000 per month for minor violations and fines up to $500,000 for violations that result in lost or stolen financial data.

**Task 3**

**3.1: Explain the methods of attack used to target encrypted data.**

**Analytic attack:**

It is an algebraic mathematical manipulation that attempts to reduce the complexity of the cryptographic algorithm. If this attack is successful, if the attacker will be able to quickly figure out how the plain text is converted to the cyphered text.

**Implementation Attack:**

Using this attack, an attacker attempts to exploits some implementation weaknesses in software, protocol or algorithms.

**Brute-Force Attack:**

Using this attack, an attacker simply tries to decrypt the data with each possible secret key and checks the result of the decryption to see if it makes sense. Given enough time and computational resources, this attack is guaranteed to work since the true secret key must be within the set of possible secret keys and the attacker will eventually try it and (hopefully) realize that the resulting plaintext is the correct one.

**Statistical Attack:**

In this Attack, an attacker exploits statistical weaknesses in a cryptosystem, such as the inability to produce true random numbers or floating-point errors caused by the cryptosystem, such as a lack of randomness when generating a key.

**Birthday Attack:**

Using the birthday attack, an attacker exploits the probability that two messages using the same hash algorithm that will produce the same message digest. So, it is exploiting collisions.

**Meet-in-the-middle Attack:**

In this attack, the plain text is encrypted with every possible key at one end, and then a cryptographic message is then decrypted with every possible key at the other end. The result of the comparison can help to discover which algorithm is used and the secret key.

**Man-in-the-middle Attack:**

This attack involves an attacker can intercept data between two parties and possibly modify it or steal confidential information such as personal details or fund transfer details. People connected on an open or public network are likely to be attacked using this attack.

**Replay Attack:**

In this attack, an attacker intercepts session keys or authentication traffic and then replays them later to authenticate and gain access. This attack can be countered.

**Ciphertext Only Attack:**

In this attack, the cryptanalyst obtains the ciphertext of several messages which are encrypted using the same encryption algorithm but may not have the associated plaintext. The cryptanalyst then attempts to decrypt the data by searching for words that are used frequently. This attack is difficult and requires a large amount of ciphertext.

**Chosen Plain Text:**

This attack involves the cryptanalyst selecting a sample of plaintext and obtains the corresponding ciphertext. Several types of chosen text attacks exist, including Chosen Ciphertext which involves the cryptanalyst choosing the ciphertext to be decrypted and the corresponding plaintext is obtained.

**Known Plaintext Attack:**

In this attack, the cryptanalyst obtains the ciphertext and corresponding plaintext of several past messages and uses it to decipher new encrypted messages.

**3.2: Assess the additional encryption methods available.**

**End-to-end encryption**

This method prevents third parties from accessing data while it is being shared from one device to another. Using this method, the data is encrypted on the sender's system or device, and only the intended recipient can decrypt it and view it in plain text but when packets are properly routed, only the data is encrypted, not the routing information.

**Link encryption**

Using this technique, a communication traveling along a network is encrypted and decrypted at every stage, or node. It is used to prevent traffic analysis and avoid human error. With link encryption, a communication is encrypted at each node such as devices and network switches.

**3.3: Explain the key principles of escrow and recovery.**

Law enforcement has always been concerned about the potential use of encryption for criminal purposes.

Key escrow is a method of storing important cryptographic keys. Each key stored in an escrow system is tied to the original user and subsequently encrypted for security purposes. Much like a valet or coat check, each key is stored in relation to the user that leverages it, and then returned once queried. By using key escrow, organizations can ensure that in the case of catastrophe, be it a security breach, lost or forgotten keys, natural disaster, or otherwise, their critical keys are safe.

**3.4: Explain the importance of having robust encryption arrangements within IT systems.**

Robust encryption keeps your valuable information safe. It is a vital tool that allows journalists to communicate securely with their sources, NGOs to protect their work in repressive countries, and lawyers to communicate privately with their clients. It protects our vital infrastructure: our communications network, the power grid and everything else. And as we move to the Internet of Things with its cars and thermostats and medical devices, all of which can destroy a person's life and property if obtained and misused by an attacker, For example, a doctor may use a medical device to get a patient's heart rate information in order to give them the right medication, so if the attacker gets in the middle of this process and changes the result that the medical device will give after the process, the doctor may give the patient wrong treatment or medication and this may result in a person losing a life, so it is very important to keep valuable information safe.

Encryption lets you protect data you send, receive, and store, regardless of device, and involves altering text to make it virtually impossible for cybercriminals to read. For example, a person may be logging into a bank account on website, and an attacker gets in the middle of this process, while the data be sent is not encrypted, the attacker will obtain this data and misuse it. Encryption allows businesses and its employees to safeguard their passwords and other sensitive information against cybercriminals.

**3.5: Evaluate the existing encryption arrangements.**

Encryption is a critical component of security, encryption is used every day, and our Internet-laced world would be a far riskier place if encryption wasn't used.

Encryption keeps you safe. Encryption protects your financial details and passwords when you bank online. It protects your cell phone conversations from eavesdroppers. Any weakness in encryption will leave a vulnerability for attackers, or criminals and by foreign governments. So having a strong encryption will ensure security.

**3.6: Design an encryption plan to meet the needs of a given organization, with recommended courses of actions:**

**1. Collaboration**

Creating an encryption plan for an organization requires a collaborative effort, a team that includes members of management, IT and operations. An organization must start by bringing together key data stakeholders and work to identify the regulations, laws, guidelines and external influences that will factor into purchasing and implementation decisions. From there, you can move on to identifying high-risk areas, such as laptops, mobile devices, wireless networks and data backups.

**2. Data classification**

Companies that don’t have an effective data classification and/or prioritization program in place, are likely to struggle with encrypting their data. Data classification policies and tools facilitate the separation of valuable information that may be targeted from less valuable information by attackers. Information is divided into predefined groups that share a common risk, and the corresponding security controls required to secure each group type are detailed. and classification tools are used to improve the treatment and handling of sensitive data, as well as to promote a culture of security that helps to enforce data governance policies and prevent inadvertent disclosure. Classification metadata can be ingested by data loss prevention (DLP), encryption and other security solutions to determine which information is sensitive and how it should be protected.

**3. Key Management**

A business or an organization should always secure their your keys and certificates, If they are not properly secured the organization is in a risk of being attacked, no matter what security controls are in place. Many organizations have tens of thousands of keys and certificates, with no clear understanding of their inventory. They do not know how keys and certificates are being used, what systems they provide access to, or who has control over them. It is imperative that organizations understand which keys and certificates are used in the network, who has access to them, and how and when they are being used. The first step in gathering this information is to gain a clear understanding of the organization’s inventory by centrally managing keys and certificates. This will enable you to detect anomalous behavior, such as rogue self-signed certificates. Critical aspects of key management include the following:

Encryption Key Lifecycle Management:

While encryption key lifecycle management can be overwhelming to organizations with many keys, there is no way to be sure of the integrity of the keys, so these keys must be protected with a reliable key management solution from the moment they are created through their lifecycle of initiation, distribution, activation, deactivation and termination.

Heterogeneous Key Management:

A centralized key management platform allows for unified access to all the encryption keys. Requiring all keys to be managed from the same place, in the same way, allows one to have a deep understanding of how the keys are being used and more importantly, whether they are being accessed incorrectly. Without an overarching heterogeneous key management solution, the organization will be continuously chasing after rogue keys and struggling to ensure encrypted data is valid and able to be decrypted when necessary. The deployment of Hardware security modules (HSMs) can help to protect the key management lifecycle in complex environments.

**Finding the Right Solution for Your Environment**

When you have established your key management needs, you evaluate and implement encryption solutions for your organization as there are many options and factors to consider. Companies should explore working with an independent partner who can help test potential solutions and find the best fit for their environment.

**Access Control**

An organization must ensure that only authorized users can access its data to prevent it from being tampered with by anyone inside or outside of the organization. A successful encryption strategy defines strong access-control techniques, using adequate combinations of file permissions, passwords, and two-factor authentication. Access controls must be audited on a regular basis to ensure their validity, for security purposes.

**Consequences**

Before deployment, an organization should write policy, endorsed by management and communicated to end-users, including business partners and third parties such as cloud service providers that handle sensitive data. If the cloud service provider cannot meet your company’s policies, then they don’t get your data. Otherwise, you will be risking, running into a compliance problem. Encryption responsibility should be fixed and carry consequences for non-compliance.