網路安全 Network Security

Midterm1

111061548 游鎮遠

1.

**YES:**

**(b) Former employees who left the company because of downsizing:**

When employees leave a company, they should no longer have access to the company's network and sensitive information. Security risks arise if former employees retain unauthorized access.

**(d) The building management company where an organization has its offices has decided to install a fire sprinkler system:**

While the installation of a fire sprinkler system itself may not pose a safety risk, any work performed by a third-party service provider on a company's premises may introduce security vulnerabilities.

**NO:**

**(a) The daily carrier personnel who drop off and picks up packages:**

Generally, industry personnel are not directly involved in the company's cybersecurity work. However, if they access sensitive areas or systems as part of their job, there are potential risks.

**(c) An employee traveling on company business to another city:**

An employee traveling for company business should not necessarily be a breach of network security. However, it's essential to ensure that employees are following security protocols and using secure networks when accessing company resources remotely.

2. 72.

DES takes a 8-octet (64-bit) plaintext block and yields a 8-octet cipherblock, CBC requires a 8-octet initialization vector (IV) to be sent along with the cipherblocks. So X now sends 64 octets of cipherblocks plus 8 octets of IV, for a total of 72 octets.

3.

i. Start with the ciphertext C, and the two keys k1 and k2.

ii. First, apply the XOR operation with k2 to the ciphertext C:

$$m' = C \oplus k_2$$

iii. Then use the key k1 to perform a standard DES decryption on the result of step 2.

$$m'' = DES\_decrypt(k_1, m')$$

iv. The final step is to apply the XOR operation between the result of step 3.

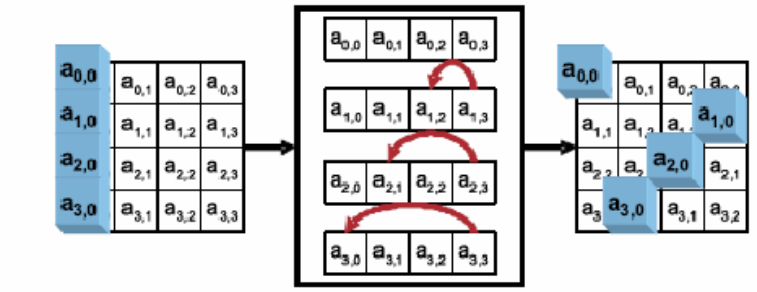
$$m = m'' \oplus k_2$$

The final result m is the decrypted original message.

4.

**Shift Rows:**

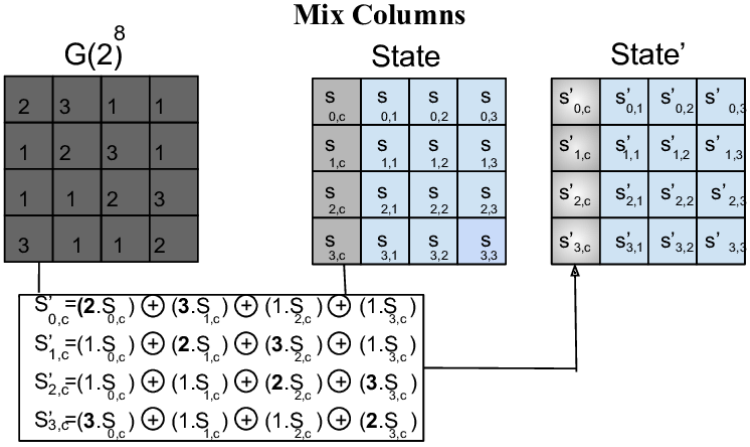
It cyclically shifts the bytes in each row by a certain offset.



(https://www.researchgate.net/figure/Shift-row-transformation_fig3_280460094)

**Substitute bytes:**

It uses a fixed table (S-box) given in design. This operation provides the non-linearity in the cipher.




(https://www.researchgate.net/figure/Sub-Bytes-step-1-Byte-Substitution-The-byte-substitution-step-consists-of-replacing_fig6_322518289)

Changing the order of operations does not weaken the security of AES (nor improve it). While Shift Rows and Substitute bytes are commutative, they are not commutative Mix Columns, so changing the order of operations won't produce the same result, but that's not relevant since we're looking at it from a security perspective.

5. (a)

**Encryption:**

i. Generate a unique counter value (ctr) for each plaintext block.

ii. Encrypt the counter value using the block cipher algorithm (e.g., AES) with the encryption key to produce a pseudorandom keystream block.

iii. XOR the obtained keystream block with the corresponding plaintext block to produce the ciphertext block.

iv. Increment the counter value and repeat the process for the next plaintext block.

$$ctrE(k, m) = IVc_1c_2 \dots c_l$$
$$c_i = E(k, IV + i - 1) \oplus \mathrm{m_i}$$

**Decryption:**

i. Generate the same counter value (ctr) used for encryption.

ii. Encrypt the counter value using the block cipher algorithm with the same encryption key to generate the same keystream block.

iii. XOR the keystream block with the ciphertext block to recover the plaintext block.

iv. Increment the counter value and repeat the process for the next ciphertext block.

$$ctrD(k, c) = m_1m_2 \dots m_l$$
$$m_i = E(k, IV + i - 1) \oplus \mathrm{c_i}$$

(b)

In CTR mode, each counter value (ctr) is used to produce a unique keystream block for XORing with a plaintext block. If there is a transmission bit error in a particular ciphertext block (ci), it will affect only that specific ciphertext block and not impact the neighboring blocks. This is a significant advantage of CTR mode, as errors are localized and do not propagate to adjacent blocks. Therefore, only one plaintext block corresponding to the affected ciphertext block will be impacted by the transmission bit error.

6. (a)
    i. Intercept message C1C2C3, which consists of three blocks: C1 for ‘fromAccount’, C2 for ‘toAccount’, and C3 for ‘amount’.
    ii. Calculate the XOR between C2 (for ‘toAccount’) and the account number (the attacker's own account number) to which he wants to transfer the money.
    iii. Construct a new message C2' by the XOR obtained in step 2, this will effectively change ‘toAccount’ to the attacker's account.
    iv. Keep C2 (for ‘toAccount’) unchanged.
    v. Construct a new message C3' (for ‘amount’) to change the amount required by the attacker.
    vi. Send the modified message C1C2’C3' to the bank.

    (b)

    The use of a Message Authentication Code (MAC) can prevent this attack by ensuring the integrity and authenticity of the message. A MAC is a cryptographic tag that is computed over the message and appended to it. In this context, it is used to verify that the message has not been tampered with during transmission.

7.

The difficulty of finding two documents with the same message digest is a fundamental requirement for the reliability and security of digital signatures. It ensures the uniqueness, integrity, and non-repudiation of digitally signed documents and prevents forgery and fraudulent activities. Cryptographically strong hash functions are specifically designed to provide this property, known as collision resistance.

8.

In the RSA algorithm, it is not possible for more than one value of d to work with a given pair of e, p, and q when RSA is correctly implemented and used as intended. This is because d, the private exponent, is uniquely determined as the multiplicative inverse of e modulo the totient of n, which is denoted as $\varphi(n)$. In mathematical terms, it can be expressed as:

$$d \equiv e^{-1} \ (mod\ \varphi(n))$$

The uniqueness of d is guaranteed modulo $\varphi(n)$, and this mathematical property ensures that there is only one valid private exponent for a given set of e, p, and q.