SECURITY / ENCRYPTION

Security: Software security is the protection of software applications and digital experiences from unauthorized access, use, or destruction. Software security solutions help ensure data is protected while in transit and at rest, and can also help protect against system vulnerabilities like malware and ransomware attacks.

Encryption: Data encryption is a security mechanism that converts your company's plaintext data into encoded information called ciphertext. The cryptic text or numbers can be decoded only with a unique key that's provided at the time of encryption.
The two main kinds of encryption are **symmetric** encryption and **asymmetric** Encryption(Public Key Encryption)

a. **Symmetric:** It uses a single key for encryption and decryption. Here, the sender must share the private key with the receiver to access the data or information.
b. **Asymmetric:** This encryption method works with two keys: one public key and one private key. The public key is shared with anyone and is used to encrypt the data. However, the private key must remain a secret key because it is used to decrypt the data or message.
c.

Industry trends and needs: There are many applications in the industry that are using end-to-end encryption strategies to provide secure means of communication for the users.
Some of them are

1. Signal
2. WhatsApp
3. Telegram
4. Threema
5. Wire

Different Encryption techniques:

1. **Advanced Encryption Standard (AES)**: This is a specification for the encryption of electronic data established by the U.S National Institute of Standards and Technology (NIST) in 2001.AES is a block cipher. It takes 128 bits as input and outputs 128 bits of encrypted cipher text as output. AES relies on the substitution-permutation network principle which means it is performed using a series of linked operations that involves replacing and shuffling the input data.

2. **Data Encryption Standard (DES)**: DES is a block cipher and encrypts data in blocks of size of 64 bits each, which means 64 bits of plain text go as the input to DES, which

produces 64 bits of ciphertext. The same algorithm and key are used for encryption and decryption, with minor differences. The key length is 56 bits.

3. **Rivest- Shamir-Adleman(RSA)**: It is an asymmetric encryption algorithm. It is based on the factorization of the product of two large prime numbers. It uses a public key and private key for securing data. The message is encrypted using the public key and the message is decrypted using the matching private key.

4. **Triple Data Encryption Standard (TDES)**: Triple DES is a symmetric encryption technique and a more advanced form of the Data Encryption Standard (DES) method that encrypts data blocks using a 56-bit key. Triple DES applies the DES cipher algorithm three times to each data block. It uses three 56 bit keys for encryption and decryption
5. **BlowFish Technique:** Blowfish is used as a replacement for a data encryption algorithm (DES). This technique uses symmetric block cryptography. The operation is performed on varying numbers of key length that ranges from 32 – 448 bits. Data is divided into chunks of 64 – bit blocks as it uses the block cipher technique, so encryption and decryption are carried out accordingly.

Pros / Cons of Current Solutions:

1. **Advanced Encryption Standard (AES):**
   a. **Pros :**
      - AES can be implemented on both hardware and software.
      - AES is implemented in a wide range of applications as it is defined as the standard by NIST.

   b. **Cons :**
      - The key used in AES if not employed properly can cause a cryptanalytic attack. Therefore, key scheduling should be done carefully
2. **Data Encryption Standard (DES):**
   a. **Pros:**
      - DES has a 56-bit key which raises the possibility of 256 possible keys which makes brute force impossible.
      - The 8 s boxes used in each round were not made public and even it is impossible for anyone to discover the design of s-boxes which makes the attack more impossible

   b. **Cons:**
      - DES was not designed for application and therefore it runs relatively slowly.
3. **Rivest- Shamir-Adleman(RSA):**
   a. **Pros:**
      - It is very easy to implement the RSA algorithm.

- Cracking the RSA algorithm is very difficult as it involves complex mathematics.
- Sharing public keys with users is easy.

b. **Cons:**

- It has a slow data transfer rate due to the large numbers involved.
- It requires a third party to verify the reliability of public keys sometimes.
- High processing is required at the receiver's end for decryption.

4. **Triple Data encryption Standard(TDES):**

a. **Pros:**

- It is very easy to modify existing software to use Triple DES.
- It also has the advantage of proven reliability and a longer key length that eliminates many of the attacks

b. **Cons:**

- It is slow, especially in software as it was designed for hardware implementations.
- It requires more processing time as it needs to apply the algorithm 3 times.

5. **BlowFish Technique:**

a. **Pros:**

- The Blowfish algorithm also has a lesser amount of operations to complete compared to other encryption algorithms
- Blowfish is a fast block cipher except when changing keys. Each new key requires a pre-processing equivalent to 4KB of text.

b. **Cons:**

- The key schedule of Blowfish takes a long time.
- This can't provide authentication as well as non-repudiation as two people have the same key.

Improvements:

The biggest challenge for using different encryption techniques is generating a strong key that cannot be regenerated by hackers and remembering or recording keys/passwords when accessing the data. Most of the algorithms use a secure cryptographic randomizer to generate keys, instead of that we can use sender/receiver biometric information like fingerprint data, facial data, and voice data in combination with random numbers to generate keys. This way the key will be more strong and it will also require additional information of biometrics in order to break the key. As biometric information comes under immediate personal data, The data can be saved with the highest security and can also be protected from misuse by very strict laws.

References:

1. https://csrc.nist.gov/projects/block-cipher-techniques
2. https://csrc.nist.gov/csrc/media/projects/key-management/documents/transitions/transitioning_cryptoalgos_070209.pdf
3. https://www.goodcore.co.uk/blog/types-of-encryption/
4. https://faq.whatsapp.com/820124435853543
5. https://signal.org/docs/specifications/xeddsa/
6. https://core.telegram.org/api/end-to-end
7. https://threema.ch/en/security
8. https://wire.com/en/product/messaging/