NAMA : PRIYO SIGIT PURNOMO

NIM : 1410652013

TI-SORE

UAS KEAMANAN INFORMASI

.....

Cryptography (kriptografi)

1. Cryptology is the science of secure communications. Cryptography creates messages whose meaning is hidden; cryptanalysis is the science of breaking encrypted messages (recovering their meaning). Many use the term cryptography in place of cryptology: it is important to remember that cryptology encompasses both cryptography and cryptanalysis. A cipher is a cryptographic algorithm. A plaintext is an unencrypted message. Encryption converts the plaintext to a ciphertext. Decryption turns a ciphertext back into a plaintext.

2. Confidentiality, integrity, authentication, and nonrepudiation. Cryptography can rovide confidentiality (secrets remain secret) and integrity (data is not altered in an unauthorized manner). Cryptography can also provide authentication (proving an identity claim). Additionally, cryptography can provide nonrepudiation, which is an assurance that a specific user performed a specific transaction and that the transaction did not change.

3. Substitution and permutation

Cryptographic substitution replaces one character for another; this provides confusion. Permutation (also called transposition) provides diffusion by rearranging the characters of the plaintext, anagram style.

4. Monoalphabetic and polyalphabetic ciphers

A monoalphabetic cipher uses one alphabet: a specific letter (like “E”) is substituted for another (like “X”). A polyalphabetic cipher uses multiple alphabets: “E” may be substituted for “X” one round and then “S” the next round.

5. Exclusive Or (XOR)

Exclusive Or (XOR) is the “secret sauce” behind modern encryption. Combining a key with a plaintext via XOR creates a ciphertext. XOR-ing to same key to the ciphertext restores the original plaintext. XOR math is fast and simple

6. Types of cryptography

There are three primary types of modern encryption: symmetric, asymmetric, andhashing. Symmetric encryption uses one key: the same key encrypts and decrypts. Asymmetric cryptography uses two keys: if you encrypt with one key, you may decrypt with the other. Hashing is a one-way cryptographic transformation using an algorithm (and no key). Cryptographic protocol governance describes the process of selecting the right method (cipher) and implementation for the right job, typically at an organization-wide scale. For example, a digital signature provides authentication and integrity, but

not confidentiality. Symmetric ciphers are primarily used for confidentiality, and AES is preferable over DES due to strength and performance reasons (which we will also discuss later)

7. Stream and block ciphers

Symmetric encryption may have stream and block modes. Stream mode means each bit is independently encrypted in a "stream." Block mode ciphers encrypt blocks of data each round: 56 bits for the Data Encryption Standard (DES) and 128, 192, or 256 bits for AES, for example. Some block ciphers can emulate stream ciphers by setting the block size to 1 bit; they are still considered block ciphers.

8. Initialization vectors and chaining

An initialization vector is used in some symmetric ciphers to ensure that the first encrypted block of data is random.

9. DES

DES is the Data Encryption Standard, which describes the Data Encryption Algorithm (DEA). IBM designed DES, based on their older Lucifer symmetric cipher. It uses a 64-bit block size (meaning it encrypts 64 bits each round) and a 56-bit key.

10. International Data Encryption Algorithm

The International Data Encryption Algorithm is a symmetric block cipher designed as an international replacement to DES. The IDEA algorithm is patented in many countries. It uses a 128-bit key and 64-bit block size.

11. ASYMMETRIC ENCRYPTION

Asymmetric encryption uses two keys: if you encrypt with one key, you may decrypt with the other. One key may be made public (called the public key); asymmetric encryption is also called public key encryption for this reason. Anyone who wants to communicate with you may simply download your publicly posted public key and use it to encrypt their plaintext. Once encrypted, your public key cannot decrypt the plaintext: only your private key can do so. As the name implies, your private key must be kept private and secure.

12. HASH FUNCTIONS

A hash function provides encryption using an algorithm and no key. They are called "one-way hash functions" because there is no way to reverse the encryption. A variable-length plaintext is "hashed" into a (typically) fixed-length hash value (often called a "message digest" or simply a "hash"). Hash functions are primarily used to provide integrity: if the hash of a plaintext changes, the plaintext itself has changed. Common older hash functions include Secure Hash Algorithm 1 (SHA-1), which creates a 160-bit hash and Message Digest 5 (MD5), which creates a 128-bit hash. Weaknesses have been found in both MD5 and SHA-1; newer alternatives such as SHA-2 are recommended.

13. CRYPTOGRAPHIC ATTACKS

Cryptographic attacks are used by cryptanalysts to recover the plaintext without the key. Please remember that recovering the key (sometimes called "steal the key") is usually easier than breaking modern encryption. This is what law enforcement typically does

when faced with a suspect using cryptography: they obtain a search warrant and attempt to recover the key.

14. Brute force

A brute-force attack generates the entire keyspace, which is every possible key. Given enough time, the plaintext will be recovered.

Known plaintext

A known plaintext attack relies on recovering and analyzing a matching plaintext and ciphertext pair: the goal is to derive the key that was used. You may be wondering why you would need the key if you already have the plaintext: recovering the key would allow you to decrypt other ciphertexts encrypted with the same key.

Chosen plaintext and adaptive-chosen plaintext

A cryptanalyst chooses the plaintext to be encrypted in a chosen plaintext attack; the goal is to derive the key. Encrypting without knowing the key is done via an "encryption oracle" or a device that encrypts without revealing the key. Adaptive-chosen plaintext begins with a chosen plaintext attack in round 1. The cryptanalyst then "adapts" further rounds of encryption based on the previous round.

Chosen ciphertext and adaptive-chosen ciphertext

Chosen ciphertext attacks mirror chosen plaintext attacks: the difference is that the cryptanalyst chooses the ciphertext to be decrypted. This attack is usually launched against asymmetric cryptosystems, where the cryptanalyst may choose public documents to decrypt that are signed (encrypted) with a user's public key. Adaptive-chosen ciphertext also mirrors its plaintext cousin: it begins with a chosen ciphertext attack in round 1. The cryptanalyst then "adapts" further rounds of decryption based on the previous round.

Meet-in-the-middle attack

A meet-in-the-middle attack encrypts on one side, decrypts on the other side, and meets in the middle. The most common attack is against "double DES," which encrypts with two keys in "encrypt, encrypt" order. The attack is a known plaintext attack: the attacker has a copy of a matching plaintext and ciphertext and seeks to recover the two keys used to encrypt.

Known key

The term "known-key attack" is misleading: if the cryptanalyst knows the key, the attack is over. Known key means the cryptanalyst knows something about the key, to reduce the efforts used to attack it. If the cryptanalyst knows that the key is anuppercase letter and a number only, other characters may be omitted in the attack.

Differential cryptanalysis

Differential cryptanalysis seeks to find the "difference" between related plaintexts that are encrypted. The plaintexts may differ by a few bits. It is usually launched as an adaptive-chosen plaintext attack: the attacker chooses the plaintext to be encrypted (but does not know the key) and then encrypts related plaintexts.

Linear cryptanalysis Linear cryptanalysis is a known plaintext attack where the cryptanalyst finds large amounts of plaintext/ciphertext pairs created with the same key.

The pairs are studied to derive information about the key used to create them. Both differential and linear analyses can be combined as differential linear analysis.

Side-channel attacks

Side-channel attacks use physical data to break a cryptosystem, such as monitoring CPU cycles or power consumption used while encrypting or decrypting.