Cryptography

A way of Texting Secretly

Cryptography

Cryptography

The field of study related to encoded information (comes from Greek word for "secret writing")

Encryption

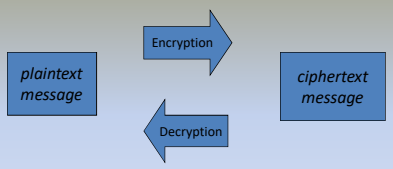
The process of converting plaintext into cipher-text

Decryption

The process of converting cipher-text into plaintext

2

Cryptography



Encrypted(Information) cannot be read

Decrypted(Encrypted(Information)) can be

3

Cryptography

Cipher

An algorithm used to encrypt and decrypt text

Key

The set of parameters that guide a cipher

Neither is any good without the other

4

Encryption / Decryption

- **Encryption**: A process of encoding a message, so that its meaning is not obvious. (= encoding, enciphering)
- **Decryption**: A process of decoding an encrypted message back into its original form. (= decoding, deciphering)
- A **cryptosystem** is a system for encryption and decryption.

5

Plaintext / ciphertext

- P: plaintext
- C: ciphertext
- E: encryption
- D: decryption
- C = E (P)
- P = D (C)
- P = D (E(P))

6

Terminology

- **Cryptography:** The practice of using encryption to conceal text. (**cryptographer**)
- **Cryptanalysis:** The study of encryption and encrypted messages, with the goal of finding the hidden meanings of the messages. (**cryptanalyst**)
- **Cryptology** = cryptography + cryptanalysis

7

Two forms of encryption

- **Substitutions**
  One letter is exchanged for another
  Examples: monoalphabetic substitution ciphers, polyalphabetic substitution ciphers
- **Transpositions (= permutations)**
  The order of the letters is rearranged
  Examples: columnar transpositions

Cryptanalysis

- The process of decrypting a message without knowing the cipher or the key used to encrypt it
- A cryptanalyst may work with various data (intercepted messages, data items known or suspected to be in a cipher-text message), known encryption algorithms, mathematical or statistical tools and techniques, properties of languages, computers, and plenty of ingenuity and luck.

1. Attempt to break a single message
2. Attempt to recognize patterns in encrypted messages
3. Attempt to find general weakness in an encryption algorithm

9

Substitution Ciphers

- A cipher that substitutes one character with another.
- These can be as simple as swapping a list, or can be based on more complex rules.
- These are NOT secure anymore, but they used to be quite common.

Caesar ciphers

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Substitute the letters in the second row for the letters in the top row to encrypt a message

Encrypt(COMPUTER) gives FRPSXWHU

Substitute the letters in the first row for the letters in the second row to decrypt a message

Decrypt(Encrypt(COMPUTER))
= Decrypt(FRPSXWHU) = COMPUTER

11

Transposition Cipher

T O D A Y
+ I S + M
O N D A Y

Write the letters in a row of five, using '+' as a blank. Encrypt by starting spiraling inward from the top left moving counter clockwise

Encrypt(TODAY IS MONDAY) gives T+ONDAYMYADOIS+

Decrypt by recreating the grid and reading the letters across the row

The key are the dimension of the grid and the route used to encrypt the data

12

Cryptosystems

- **Symmetric** encryption:
  P = D (*Key*, E(*Key*,P))
- **Asymmetric** encryption:
  P = D (Key_D, E(Key_E,P))
- **Symmetric cryptosystem**: A cryptosystem that uses symmetric encryption.
- **Asymmetric cryptosystem:** A cryptosystem that uses Asymmetric encryption.

13

Encryption on computers

- Roughly speaking, there are two different broad types of encryption that are used on computers today
  - Symmetric encryption relies on keeping keys totally secret
  - Asymmetric encryption actually publicizes one key, but keeps some information private also
- Neither is really "better" - they just use different principles.
- In reality, both are vulnerable to attacks.

Secret Key Encryption

- Secret-key ciphers generally fall into one of two categories:
  - **Stream Ciphers:** A stream cipher applies the key and algorithm one bit at a time.
  - **Block Ciphers:** A block cipher applies a private key and algorithm to a block of data simultaneously.

Symmetric Cryptography

- In cryptography, a private key (secret key) is a variable that is used with an algorithm to encrypt and decrypt code.
- It is also known as private key encryption, uses the same private key for both encryption and decryption. The risk in this system is that if either party loses the key or the key is intercepted, the system is broken and messages cannot be exchanged securely.

Asymmetric Cryptography

- It is also known as public key encryption, uses two different but mathematically linked keys. The complexity and length of the private key determine how feasible it is for an interloper to carry out a brute force attack and try out different keys until the right one is found. The challenge for this system is that significant computing resources are required to create long, strong private keys.

Secret Key Algorithm

- A secret key algorithm (sometimes called a*symmetric* algorithm) is a cryptographic algorithm that uses the same key to encrypt and decrypt data. The best known algorithm is the U.S. Department of Defense's Data Encryption Standard (DES). DES, which was developed at IBM in 1977, was thought to be so difficult to break that the U.S. government restricted its exportation.

RSA

- In 1977, Rivest, Shamir, and Adleman came up with another way to use public key cryptography
- Rather than secure key exchanges, this one actually lets you encrypt whole messages
- Today, this is the most commonly used public key cryptosystem on the market

Query Session

WKDQN BRK