Table of Content

- Security requirements and functions and related use of encryption technologies
- Cryptography basics
  - Symmetric key encryption
  - Asymmetric key encryption

Requirements

- **Confidentiality**: Ensuring that information is accessible only to those authorized to have access.
- **Integrity**: Maintaining data validity against malicious or accidental alteration.
- **Accountability**: Holding a subject accountable for her actions/results.
- **Privacy**: Protecting the data object from being seen by unauthorized users.
- **Availability**: Maintaining the resource/service deliverable to intended users.
A cryptosystem is characterized by:
- The type of encryption operations used
  - substitution / transposition
- The number of keys used
  - single-key (or private) / two-key (or public-key)
- The way in which plaintext is processed
  - block / stream

Encryption - terminology
- \( P \): plaintext - the original message/data
- \( C \): ciphertext - the coded message/data
- \( E \): cipher - algorithm for transforming plaintext to ciphertext
- \( K \): key - info used in cipher known only to sender/receiver
- encipher (encrypt) - converting plaintext to ciphertext
  - Represented as \( E_K \)
- decipher (decrypt) - obtaining plaintext from ciphertext
  - Represented as \( D_K \)
- Cryptosystem – a system for encryption/decryption

Cryptography - basics
- Cryptography - study of encryption principles/methods (how to create secret codes)
- Cryptanalysis/codebreaking - the study of principles/methods of deciphering ciphertext
  - Objective: evaluate if the cryptosystem is vulnerable
- Kerkhoffs’ principle – cryptanalysis assumes that the adversary knows the encryption/decryption algorithm but not the key
Types of Cryptanalytic Attacks

- Goal of cryptanalytic attacks:
  - Obtain the plaintext and/or the key
- Assumption: the cipher algorithm is known
- Classification according to prior knowledge:
  - ciphertext only – the cryptanalyst has access only to a collection of ciphertexts and tries to derive the key and the plaintext
  - known plaintext - the attacker has a set of ciphertexts and he knows the corresponding plaintexts.

Cypherext-only attacks
brute force search

- Algorithm and the list of all possible keys are known
- always possible to simply try every key
- most basic attack, proportional to key size
- assume either know / recognise plaintext

<table>
<thead>
<tr>
<th>Key Size (bits)</th>
<th>Number of Alternative Keys</th>
<th>Time required at 1 encryption/keys</th>
<th>Time required at 10^9 encryption/keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>56</td>
<td>$2^{56}$</td>
<td>3.5 weeks</td>
<td>1611.75 years</td>
</tr>
<tr>
<td>64</td>
<td>$2^{64}$</td>
<td>2 years</td>
<td>1011.75 years</td>
</tr>
<tr>
<td>128</td>
<td>$2^{128}$</td>
<td>2^31 years</td>
<td>1.3 x 10^21 years</td>
</tr>
<tr>
<td>192</td>
<td>$2^{192}$</td>
<td>2^31 years</td>
<td>1.3 x 10^21 years</td>
</tr>
<tr>
<td>256</td>
<td>$2^{256}$</td>
<td>2^31 years</td>
<td>1.3 x 10^21 years</td>
</tr>
</tbody>
</table>

Encryption

- Two modes:
  - Symmetric encryption
    - Also referred to as secret-key encryption
    - the only way of encrypting data until the 70s
    - Encryption/decryption algorithms use the same key
    - Key must be kept secret
    - Key distribution is very difficult
  - Asymmetric encryption
    - Also referred to as asymmetric encryption
    - Encryption key different from decryption key
    - Cannot derive decryption key from encryption key
    - Higher cost than symmetric encryption

Symmetric Encryption

Symmetric encryption provides confidentiality of the encrypted data
Symmetric Encryption

- Symmetric encryption (also known as private/secret/single key) cryptography uses one key shared by both sender and receiver:
  - if this key is disclosed communications are compromised
  - the secret key is known to both parties:
    - hence symmetric encryption does not protect sender from receiver forging a message & claiming it was sent by sender
- The mechanism does not scale as the number of parties increases: for n users \((n \times (n-1))/2\) keys are needed
- Secure key distribution is an issue

Symmetric Encryption requirements

- Two requirements for secure use of symmetric encryption:
  - R1: a strong encryption algorithm
  - R2: the secret key is known only to sender / receiver
    \[
    C = E_k(P) \quad P = D_k(C)
    \]
- Assumption: encryption algorithm is known
- Requirement R2 implies a secure channel to distribute key

Symmetric Encryption

Classical Ciphers

- Encryption mechanisms:
  - Substitution:
    - replace one basic unit (letter/byte) with another
    - maintains the order of the basic units in the plaintext but changes their identity
  - Transposition:
    - rearrange the order of basic units (letters/bytes/bits) without altering their actual values

Substitution cipher

Caesar Cipher

- Earliest known substitution cipher
- First attested use in military affairs by Julius Caesar
- It replaces each letter by 3rd following letter
- Example:
  - meet me after the toga party
  - **PHHW** **PH DIWHU** **WKH** **WRJD** **SDUWB**
Caesar Cipher

- You can define the transformation as:
  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
  DEFGHIJKLMNOPQRSTUVWXYZ

- Or you mathematically assign a number to each letter:
  a b c d e f g h i j k l m
  0 1 2 3 4 5 6 7 8 9 10 11 12
  n o p q r s t u v w x y z
  13 14 15 16 17 18 19 20 21 22 23 24 25

- then the Caesar cipher is defined by:
  \[ C = E(p) = (p + k) \mod 26 \]
  \[ p = D(C) = (C - k) \mod 26 \]

Caesar Cipher – Example

- Original plaintext: howdy
- Assigning numbers to letters:
  – howdy \rightarrow 7 14 22 3 24
- K = 5
- Apply function \( E(p) = (p + 5) \mod 26 \) to each digit:
  – 12 19 1 8 3
- Obtain letters from numbers:
  – M T B I D

Polyalphabetic Substitution Ciphers

- Main weakness of monoalphabetic substitution ciphers
  – Each letter in the ciphertext corresponds to only one letter in the plaintext letter
- Idea for a stronger cipher (1460’s by Alberti)
  – Use more than one cipher alphabet, and switch between them when encrypting different letters
- Developed into a practical cipher by Vigenère (published in 1586)

The Vigenère Cypher

- The cypher is based on using successively shifted alphabets, a different shifted alphabet for each of the 26 English letters.
- The procedure is based on the tableau shown here
- The letters of a key determine the shifted alphabets used in the encoding process
The Vigenère Cypher

Example

Plaintext: CRYPTOGRAPHY
Key: LUCKLUCKLUCK
Ciphertext: NLAZEBLJJI

• Vigenère masks the frequency with which a character appears in a language: one letter in the ciphertext corresponds to multiple letters in the plaintext. Make the use of frequency analysis more difficult.

• Any message encrypted by a Vigenère cipher is a collection of as many shift ciphers as letters in the key.

Elements of cryptanalysis

– Find the length of the key
– Divide the message into many substitution cyphertexts
– Use frequency analysis to solve the resulting cyphertexts
– One approach to find the key length is the Kasisky test – it takes advantage of the fact that common words (like ‘the’) it is inevitable that some of the four encipherments will be repeated in the ciphertext

Finding the key length

1. Look for repeated groups of letters and counts the number of letters between the beginning of each repeated group. For instance if the ciphertext was FGXTHAOWNFGXO, the distance between FGX’s is 10. Repeat this step for as many repeated groups as appear in the text.

2. Factor each of these numbers. If any number is repeated in the majority of these factorings, this is probably the length of the keyword. This is because repeated groups can appear by coincidence, but are much more likely to occur when the same letters are encrypted using the same key letters. The key letters are repeated at multiples of the key length, so the distances found in step 1 are likely to be multiples of the key length.

Example

• Moonsunstarsmoonsunsmooth
  • Key: alfa
  • MZTNFSSTLWSMZTNFSMSMTTHSWW
• Distances between repeating strings
  – MZT 12, 8
  – SFS 12
• Key length divides 8 and 12; it is thus either 2 or 4
### One-Time Pad

- Key is chosen randomly
- Plaintext $X = (x_1, x_2, \ldots, x_n)$
- Key $K = (k_1, k_2, \ldots, k_n)$
- Cyphertext $Y = (y_1, y_2, \ldots, y_n)$

\[
e_k(X) = (x_1+k_1, x_2+k_2, \ldots, x_n+k_n) \mod m
\]
\[
d_k(X) = (y_1-k_1, y_2-k_2, \ldots, y_n-k_n) \mod m
\]

### The Binary Version of One-Time Pad

Plaintext space = ciphertext space = keyspace = $\{0,1\}^n$

Key is chosen randomly

Example:
- plaintext 11011011
- key 01101001
- cyphertext 10110010

### Transposition Ciphers

**Example: Rail Fence Cipher**

- **STEP1:** Write message letters out diagonally over a number $n$ of rows
- **STEP 2:** Then read off cipher row by row

**Example**
- Original Message: meet me after the toga party
- STEP1 transforms the message into: mematrhtgpy etefeteoaat
- **STEP2:** ciphertext mematrhtgpyetefeteoaat
Symmetric encryption standards

- **DES** – Data Encryption Standard
  - adopted in 1977 by NBS (now NIST) as FIPS PUB 46
  - controversy over its security
  - Strength of DES: with a 128 bits key, it takes 1018 years to break the cipher
- **TDES** - Triple DES –
  - based on TDEA algorithm (3 keys and 3 different executions of DES)
- **AES** – Advanced Encryption Standard
  - Approved in 2001 as FIPS 197

Symmetric encryption standards

- **IDEA** (128-bit keys)
- **Blowfish** (Schneier, up to 448-bit keys)