1.1 Modern Cryptography

- The scientific study of techinques for securing digital information, transactions, and distributed computations

- We will begin with classical cryptography to understand intuition and why the modern approach is more rigourous.

1.2 The Setting of Private-Key Encryption

- classical Cryptography was concerned withe the construction of ciphers (encryption schemes)

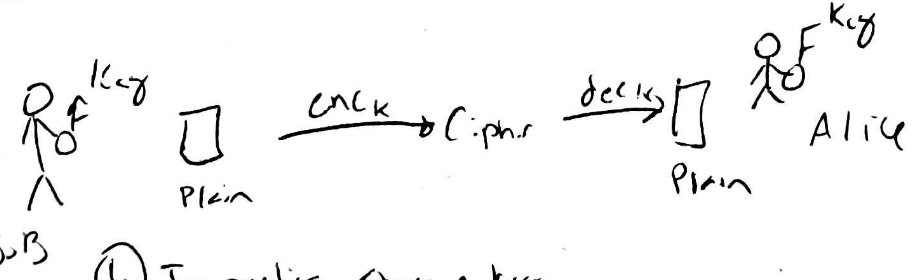
- Communicating parties share secret information in advance, This is the private key (symmetric key) setting.

① Questions Online
② review notes
③ Make Q

~~Questions~~ ✓
~~Programming p~~
~~Hex ASCII~~ ✓

Watch videos
Make next n

①



1. Two parties share a key
2. A party uses the key to encrypt - cipher text
3. Other party uses key to decrypt - plain tex
4. Both parties have same key, hence Symmetric Key Setting
5. Private Key Setting is Classical

Syntax of encryption   here is the definition

Definition

- A private key scheme is comprised of the following three Algorithms

① Key-generation algo = Gen

② Eryption Algorithm = $Enc_K(m)$

Inputs: key K, plaintext M

Outputs: Cipher text C

③ Decryption Algorithm = $Dec_K(m)$

Input: key K, Cipher text c

Output: plain text m or error

- Key space - Set of all possible keys

- ~~Plaintext Scheme~~ - Set of all possible plain text message
message space

- Correctness requirement :: For all $k \in K$ and $m \in M$

$$Dec_K(Enc_K(M)) = M$$

Lets look at a historical example of a encryption scheme called the Shift cipher.

Shifte cipher

Suppose you have any englist word M. (message space)

Associate a with 0; b with 1, ..., z with 25

$K \in \{0, \ldots, 25\}$ Key space

$Enc_K(m)$ is defined by shifting every letter of the plain text by K positions modulo 26.

$Enc_K(M) = C$ where $C_i = m_i$

$Dec_K(m)$ is defined by shifting every letter of the plain text by K positions in reverse modulo 26.

Example What is the encryption of

m = "hello"

K = "e"

~~hello~~
~~eeeee~~

m = "abc"

K = "e"

$Enc_K(m) =$ "efg"

$$\begin{array}{ccc} a & b & c \\ e & e & e \\ \hline e & f & g \end{array} \qquad \begin{array}{ccc} 0 & 1 & 2 \\ 4 & 4 & 4 \\ \hline 4 & 5 & 6 \end{array}$$

What is the decryption of Enc "efg" = c ?

$$\begin{array}{rrr} e & f & g \\ -\,e & e & e \end{array} \qquad \begin{array}{rrr} 4 & 5 & 6 \\ -4 & -4 & -4 \\ \hline 0 & 1 & 2 \end{array}$$

$Dec_k(c) =$ "abc"

As a reminder remember that

- $X = x' \bmod N$ if and only if N divides $X - x'$
- We will refer to the remainder of a number x divided by n as follows

$[x \bmod N]$ = The remainder when x is divided by N

Example

$105 = 95 \bmod 10$ $\qquad 105 \neq [95 \bmod 10]$

$105 = 5 \bmod 10$ $\qquad 5 = [95 \bmod 10]$

Example. What is the cipher text of the message "hi" with Key z?

h i	7 8
z z	25 25

We can formally define the shift cipher now.

$M = \{$ strings of lowercase English alphabet $\}$

Gen: choose $K \in \{0, \dots, 25\}$

$\mathrm{Enc}_K(m_1 \cdots m_t) = c_1 \cdots c_t$ where $c_i = [m_i + k \bmod 26]$

$\mathrm{Dec}_K(c_1 \cdots c_t] = [m_1 \cdots m_t$ where $m_i = [c_i - k \bmod 26]$

Is the shift cipher secure?

1. No, given a cipher text we can try every key
2. If text is long enough only 1 possibility will make sense

Try Q1 + Q2

Historical Ciphers and their Cryptanalysis

This is one example that

1. Highlight weakness of an ad-hoc approach. to motivate a rigourous approach

We will use this

and it

2. Demonstrate that simple approaches to achieving secure encryption are unlikely to succeed

We will see a few more classical ciphers that may appear secure at first but are not!

3. - Caesar cipher

   - shift cipher

     - weak to brute force

One thing we can conclude is that we need our key space to be large enough so that our ~~attacks~~ brute force attacks do not work

4. Sufficent Key space principle

Any secure encryption scheme must have a key space that is not vulnerable to exhaustive search

5. Necessary condition but not sufficent.

Keys and Kerckoff's principle

* Anoter thing we can conclude is the

(1.) Encryption scheme should not be keep secrect, the keys should constitute the secret information shared by the communicating parties.

Why? Because it is easier to keep a secret key than a secret algorithm

(2.) Kerckhoff's principle demands that security rely solely on the secrecy of the key

(3) A system must be practically, if not mathematically, indecipherable. (Cryptographic schemes can be broken given enough time)

(4.) Four type of attacks

- Cipher-only attack - Attacker only has ciphertext. Goal of attacker is to determine plaintext
- Known-plaintext - Attacker has one/more pair of Plaintext-ciphertext
- Choosen-plaintext
- Choosen ciphertext

Kerckhoff's Principle

" Security must relay solely on the secrecy of the key "

(1.) easier to replace key

(2.) easier to maintain secrecy of key than algorithm

Now let's introduce a encryption scheme that cannot be broken by an exhaustion search! Maybe this will be secure

Vigenere Cipher

Message space = {Strings of lower case english words}

Key space = Message space

$\mathrm{Enc}_{K_1 \dots K_n}(m_1, \dots, m_\ell) = c_1 \cdots c_\ell$ where $c_i = [m_i + k_i \bmod 26]$

$\mathrm{Dec}_{K_1 \dots K_n}(c_1 \cdots c_\ell) = m_1 \cdots m_\ell$ where $m_i = [c_i - k_i \bmod 26]$

- Encryption just shifts each character of the plaintext by the amount dictated by the next character of the key.

- Decryption reverses the process

Ex. Encrypt m = "hello" with the key "ad" using vigenere cipher.

a	b	c	...
0	1	2	...

hello	7	4	11	11	13
adada	0	3	0	3	0
hhlpo	7	7	11	14	13

Ex. 3. here

Size of the Key space is 26^n For a key of length n. For large keys this is to large to use brute force

for example $26^{14} \approx 2^{66}$, 2^{58} seconds is the estimated seconds from the big bag.

Is the Vigener cipher secure?

No, lets show why!

The vigener cipher can be thought have as a shift cipher for each position in the length of the key. Therefore we want to find the 1

1. Key length
2. Charaters in the key

B/c if we have the key them we know how to decrypt.

assumptions

(1) We know the advusery is using the Vigenere cipher.

(2) Cipher text is sufficiently long.

Fact 1. The frequency of english letters in text follow certian Probabilities. (We will

$p_0(A) = 8.2$

$p_1(B) \approx 1.6$

$P(c) \approx 3.0$

$\vdots$

$P_{25}(z) \approx .1$

Let p_i, for $0 \leq i \leq 25$ denote the probability of the ith letter in a norml text. The we have the following sum

$$\sum_{i=0}^{25} p_i^2 \approx .065$$

.065 is an invariant that tells us we have a Plain english text!

(1)

- Let q_i denote the probability the ith letter in the ciphertext.

- If the Key is k then $q_{i+k} \approx p_i$ for all i

- Assme know the lngth of the key is l. $k = k_1 k_2 \cdots k_n$

- Then $C_1, C_{1+2l}, \dots, C_{1+3l}, \dots$ are shifted by the same amount.

$\underline{h}e\underline{l}l\underline{0}$

ababa

- let q_i denote the frequency of the english letters C_1, C_{1+l} appear in the ciphertext.

- if the shift here is k_j then $q_{i+k_j} \approx p_i$

- Define

$$I_j = \sum_{i=0}^{25} p_i \, q_{i+k_j}$$

10

- If k_j is the correct shift then $I_j \approx .0065$
- Compute Each I_j. Closest to .0065 is solution

When t = length of the Key then the Sequence

$p_0, \dots, p_{25}$ is the sequence $q_0, \dots, q_{25}$ ~~[illegible]~~

with some permutation.

Therefore compute ~~[illegible]~~ I_t.

The I_t closest to .0065 will give the length

of the Key.

Summary.

1. Vigenere cipher is not secure!
2. Given a large enough message or Key we can crack it
3. Smaller messages/Keys are susceptable to brute force!

Motivation. How can we know if an encryption is secure?

- Define Security

Hexadecimal, Binary

① hexadecimal is a way of describing integers using base 16.

② hex digits 0-9 correspond to the values 0 9 and hex digit 10-15 correspond to the values A-F (WS)

③ hexadecimal numbers also correspond to bits, nibbles, and bits

④ Definition: A bit is a binary digit that is represented by 0, 1.

⑤ Definition: A nibble is four bits:

⑥ Definition: A byte is 8 bits.

hexadecimal ⟷ Binary ⟷ Base 10

Worksheet

⑦ From the worksheet you can see the correspondence between hexadecimal to binary

⑧ Lets review how to convert binary to Base 10

Binary ↔ Base 10.

① Given a binary number

$$b_{n-1} b_{n-2} \cdots b_1 b_0$$

② We convert by the formula

$$\sum_{i=0}^{n-1} b_i 2^i$$

Example.

Convert the binary number 101101 to decimal

$$= 1\cdot 2^5 + 0\cdot 2^4 + 1\, 2^3 + 1\, 2^2 + 0\cdot 2^1 + 1\cdot 2^0$$

$$= 2^5 + 2^3 + 2^2 + 1$$

$$= 32 + 8 + 4 + 1$$

$$= 45$$

Ex

Convert the hexidcimal number 0x a1b into Binary and into decimal.

Binary 0x a1b.

Each position corresponds to a nibble

a 1 b $\xrightarrow{\text{decimal}}$ a 1 b

1010 0001 1011] Binary

$$a\times16^2+1\times16^1+b\times16^0$$

$$\boxed{10\times16^2+16+11}$$

↓ decimal

$$\boxed{2^{11}+2^9+2^4+2^3+2^1+2^0}$$

Alternative Hexadecimal ↔ decimal

Given hex number

$$0x\ h_{n-1}\cdots h_0$$

We convert by the formula

$$\sum_{i=0}^{n-1} h_i' \, 16^i$$

where h_i' is h_i converted to decimal