Mathematical Puzzles, Games and Other Diversions

Day 19

Derrick Chung

April 16, 2020

Notes

Review

Summary of Basic Cryptosystems

So far, we've examined mono-alphabetic substitution ciphers. They have severe drawbacks:

- Small key space (easy to brute force)
- Completely defeated by known plaintext attacks
- Very succeptible to frequency analysis

There are ways to mitigate all these problems:

- Use a polygraphic substitution cipher (e.g. Hill cipher)
- Use a poly-alphabetic substitution cipher (e.g. Vigenere)
- Use a one-time pad*

Notes

The One-Time Pad

A Simple One-Time Pad

To transmit a message M of length n, you need a random secret key of the same length. Then add the message and key together modulo 26 (letter by letter) to get your encrypted message.

Example

Suppose Alice wants to transmit a 5-letter message HELLO to Bob using WNTAD as their shared key.

- Convert to numbers: HELLO: 8 5 12 12 15
WNTAD: 23 14 20 1 4
- Add them up (mod 26): 5 19 6 13 9
- Convert the numbers back to letters: ESFMI

To decrypt, simply **subtract** the key from the encrypted message, i.e. ESFMI - WNTAD (mod 26) = HELLO.

Notes

The One-Time Pad (cont.)

Definition

Exclusive OR (XOR) is a logical operation on two binary inputs that outputs TRUE only when the inputs are different, i.e. one is TRUE, and one is FALSE.

For our purposes, 1 = TRUE and 0 = FALSE.

p	q	$p \oplus q$
T	T	F
T	F	T
F	T	T
F	F	F

p	q	$p \oplus q$
1	1	0
1	0	1
0	1	1
0	0	0

So XOR is just addition modulo 2.

Important Note

Every message can be written in binary form,
i.e. a sequence of zeroes and ones like 01101.

Notes

The One-Time Pad (cont.)

The Standard One-Time Pad

To transmit a message M of length n, you need a random secret key of equal length. XOR the two to get your encrypted message.

Example

Suppose Alice wants to transmit a 110010101 to Bob using 001110100 as their shared key.

To encrypt, XOR the two sequences:

$$\begin{array}{rr} & 110010101 \\ \oplus & 001110100 \\ \hline & 111100001 \end{array}$$

To decrypt, XOR the encrypted message 11110001, XOR it with the shared key 001110100.

This gives you back your original message:

$$\begin{array}{rr} & 111100001 \\ \oplus & 001110100 \\ \hline & 110010101 \end{array}$$

Notes

The One-Time Pad (cont.)

Advantages

- The one-time pad is *information-theoretically* secure.
- It's easy to understand and implement.
- Encrypting and decrypting can be done by hand.
- It can be used for superencryption.
- It's practical when two parties can start off in a common secure environment, but then must be separated.

Disadvantages

- The randomness requirement is non-trivial.
- It requires a shared key between the sender and receiver.
- The length of the key must be as long as the message.
- The key can only be used once to remain secure.
- No message authentication.

Notes

A Puzzling Correspondence

Question

While in isolation, Alice is trying to mail a special package to Bob to the other side of the country. Unfortunately in their country, anything that isn't enclosed in a padlocked box is stolen before reaching the receiver.

As such, every person (including Alice and Bob) has boxes that can be padlocked as many times as they want, and as many padlocks as they need. However, neither Bob nor Alice has keys to the other's padlocks.

How can Alice safely send the package to Bob?

Notes