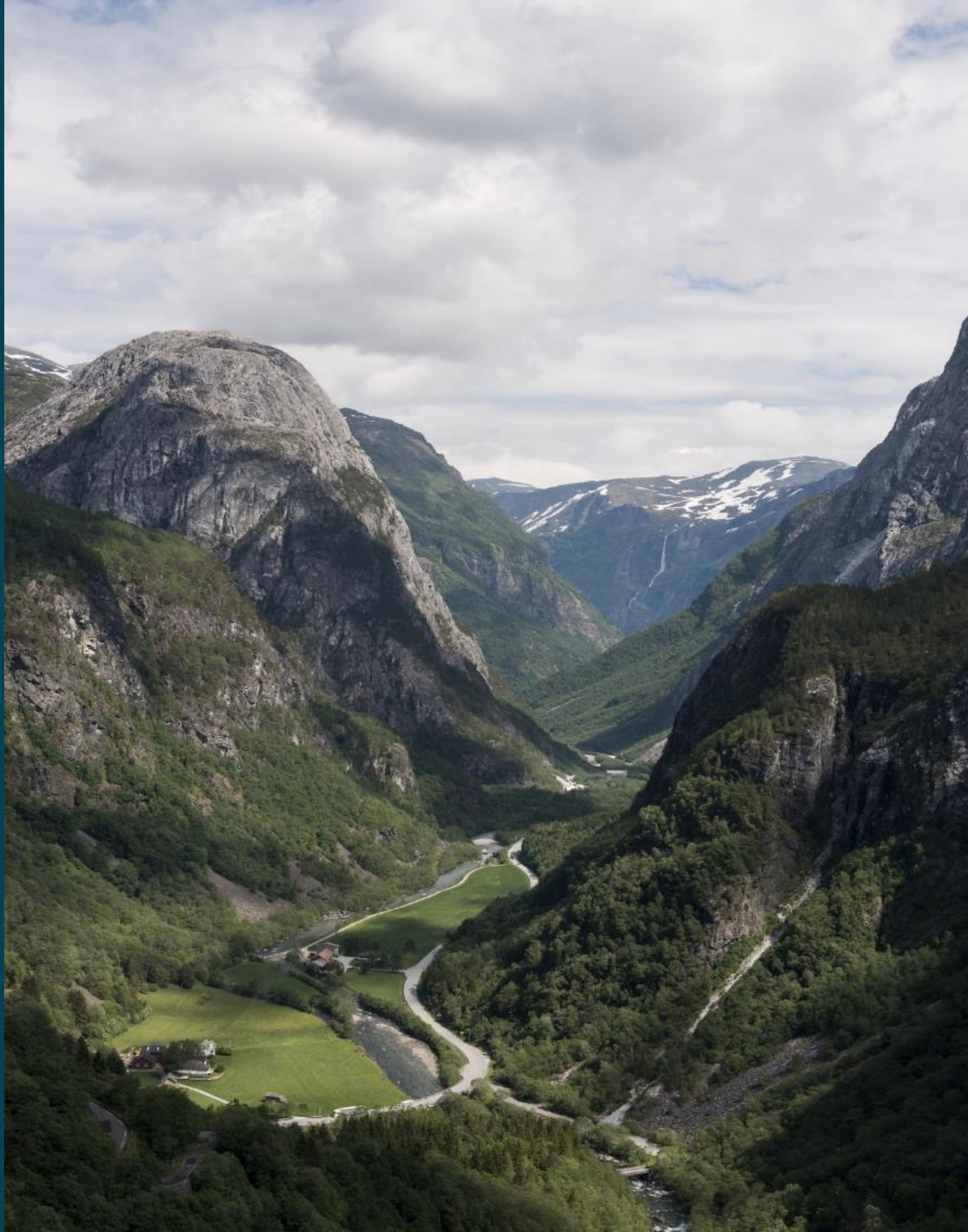
Høgskulen på Vestlandet

2. Cryptography I :
Overview of Cryptography and Applications

ELE130

Nettverkssikkerhet

Guang Yang
Bergen



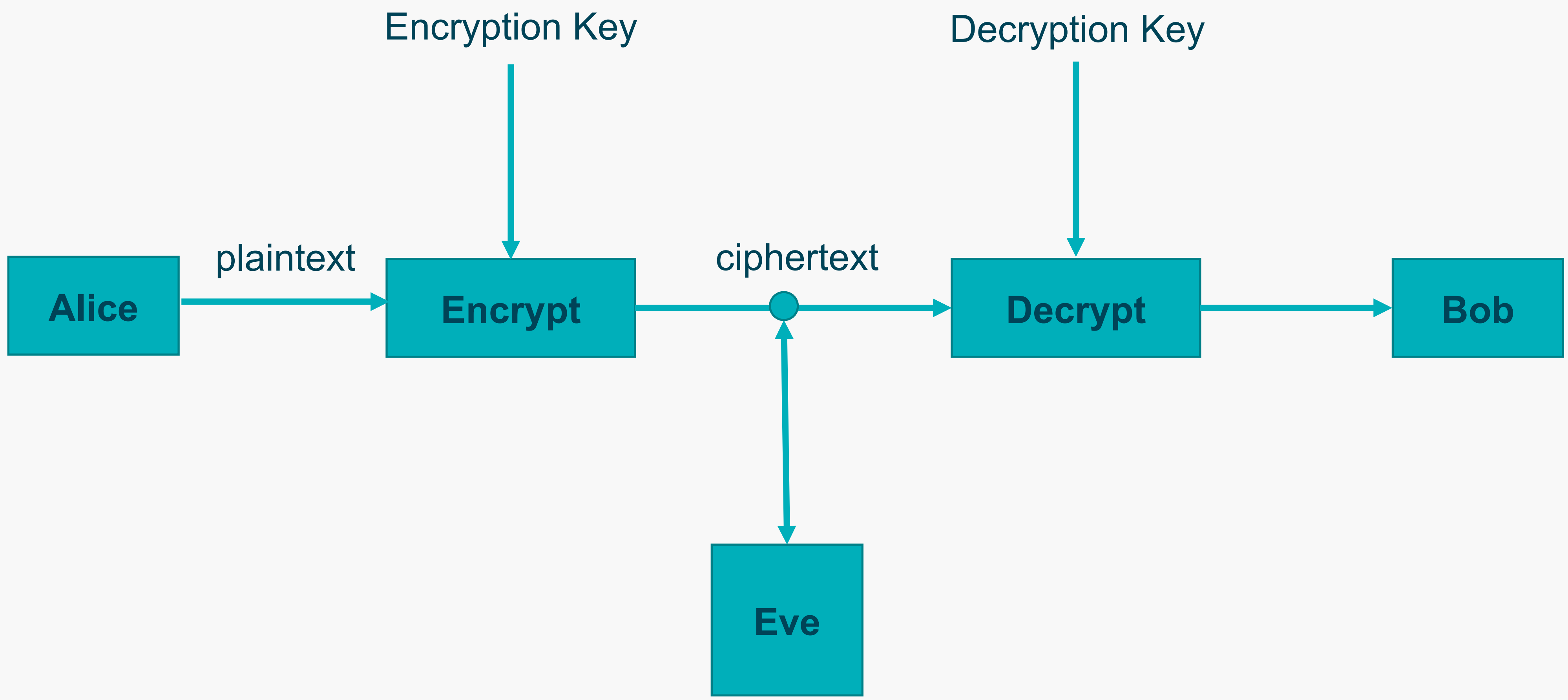
Outline

- Overview of Cryptography
- Cryptographic Applications
- Classical Cryptosystems
  - Substitution
  - Transposition

Introduction

- The techniques need to protect data belong the the field of cryptography.
- The process pf designing systems to do this is called **cryptography**
- **Cryptanalysis** deals with breaking such system
- **Cryptology** is the all-inclusive term for the study of communication over nonsecure channels, and related problems

Secure Communication



Secure Communication

Eve has one of the following goals:

1. Read the message.
2. Find the key and thus read all messages encrypted with that key.
3. Corrupt Alice’s message into another message in such a way that Bob will think Alice sent the altered message.
4. Masquerade as Alice, and thus communicate with Bob who believes he is communicating with Alice.

Which case we’re in depends on how evil Eve is.
Case 3, and 4 related to issues of integrity and authentication, respectively.

Possible Attacks

- Ciphertext only
- Known plaintext
- Chosen plaintext
- Chosen ciphertext

Kerckhoff’s principle: In assessing the security of a cryptosystem, one should always assume the enemy knows the method being used.

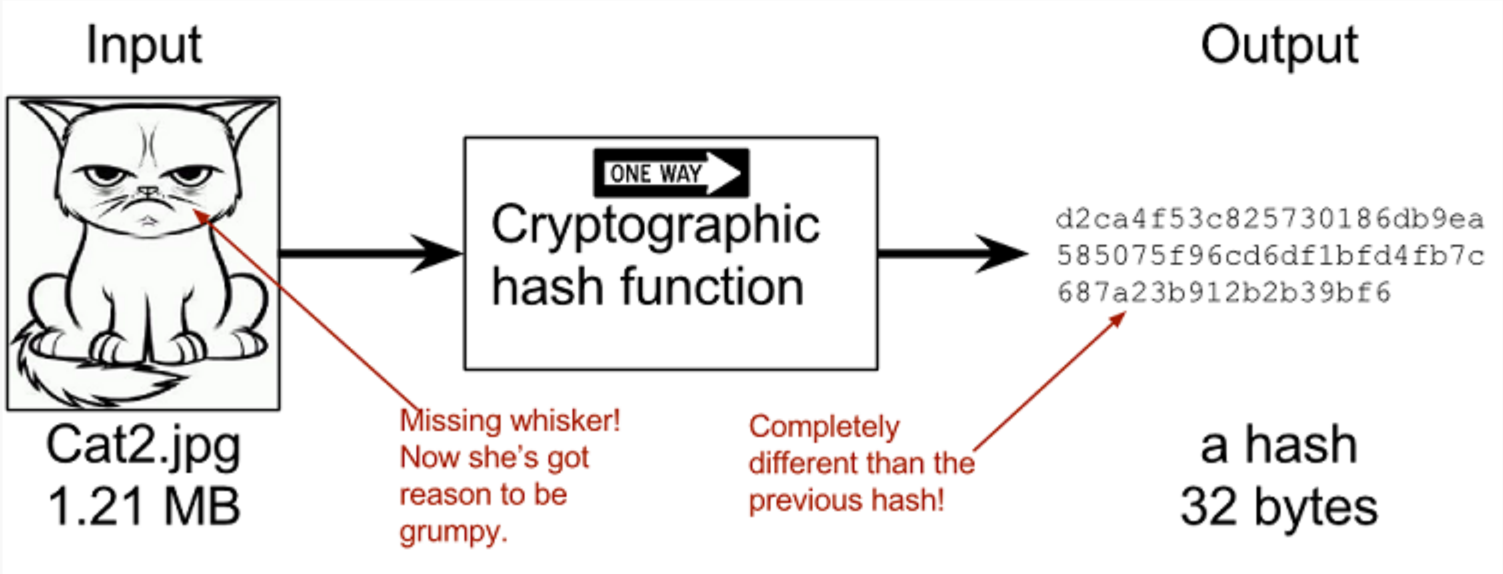
Cryptographic Applications

Cryptography is not only about encrypting and decrypting messages. It is also about solving real-world problems that require information security. There are four main objectives:

- **Confidentiality:** Eve should not be able to read Alice’s message to Bob.
- **Data Integrity:** Bob wants to be sure that Alice’s message has not been altered.
- **Authentication:** Bob wants to be sure that only Alice could have sent the message he received: **entity authentication** and **data-origin authentication**.
- **Non-repudiation:** Alice cannot claim she did not send the message.

Cryptographic Applications

- Digital signatures
- Identification
- Key establishment
- Secret sharing
- Security protocols
- Electronic cash
- Games


Input
Output
ONE WAY
Cryptographic hash function
d2ca4f53c825730186db9ea
585075f96cd6df1bfd4fb7c
687a23b912b2b39bf6
Cat2.jpg
1.21 MB
Missing whisker! Now she's got reason to be grumpy.
Completely different than the previous hash!
a hash
32 bytes

Classical Cryptosystems

Some of the older cryptosystems that were primarily used before the advent of the computer. These cryptosystems are too weak to be of much use today, especially with computers at our disposal, but they give good illustrations of several of the important ideas of cryptology.

- **Substitution**
  - Shift Cipher
  - Permutation
  - Playfair Cipher
  - One-time Pad
  - Block Cipher
- **Transposition**
- **Rotor Machine**

Substitution Ciphers: Caesar Cipher

- Julius Caesar wanted send a plaintext:

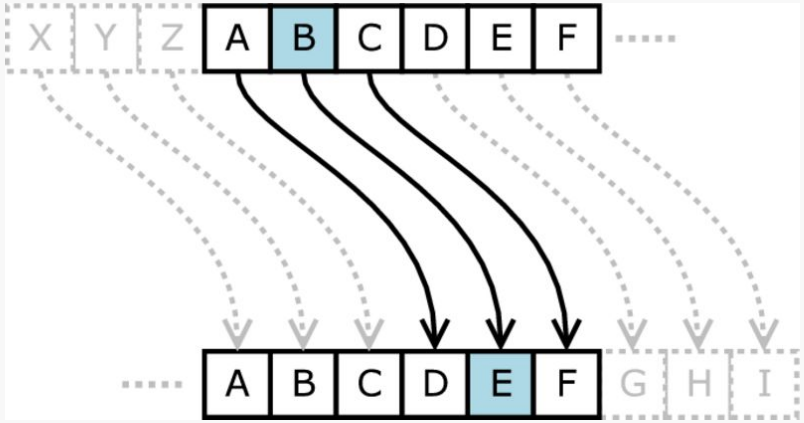
Gaul is divided into three parts

- He didn't want Brutus to read it, thus he shifted each letter by three places, the ciphertext was then:

JDXOLVGLYLGHGLQWRWKUHHSDUWV

Decryption was accomplished by shifting back by three spaces (and trying to figure out how to put the spaces back in)

- The encryption process is: $x \longmapsto x + \kappa \ (mod\ 26)$
- The decryption process is: $x \longmapsto x - \kappa \ (mod\ 26)$
- The key is an integer κ with $0 \leq \kappa \leq 25$.
- Caesar used κ = 3



Substitution Ciphers: Caesar Cipher

How the four types of attack work:

- **Ciphertext Only:**
  - Exhaustive search (only 25 keys to try);
  - If message is sufficiently long, do a frequency count (language of plaintext is known).
- **Known Plaintext:** if know just one letter of the plaintext along with the corresponding letter of ciphertext, the key can be deduced.
- **Chosen Plaintext:** choose the letter a as the plaintext. The ciphertext gives the key.
- **Chosen Ciphertext:** choose the letter A as ciphertext. The plaintext is the negative of the key.

Substitution Ciphers: Permutation

- A **permutation** of a finite set of elements S is an ordered sequence of all the elements of S, with each element appearing exactly once.
- Example: if S = {a,b,c}, there are 6 permutations of S:

  abc, acb, bac, bca, cab, cba
- In general, there are **n!** permutations of a set of **n** elements.
- For Caesar cipher, will be 26! $\approx 4\times10^{26}$ possible keys.

Substitution Ciphers: Permutation

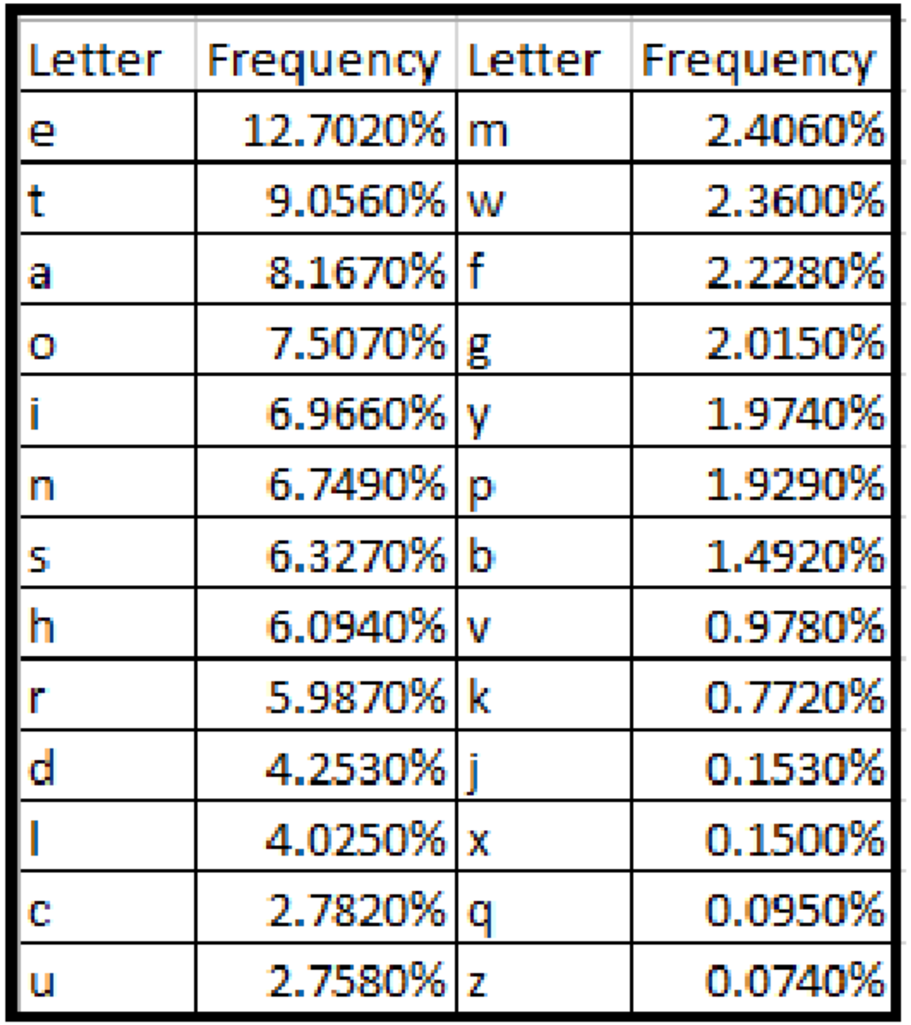
Attack:

- By the nature of language:
  1. Frequency distribution
  2. Digrams

  A simple frequency count is **not** enough to decide which is which, e.g, ***t,a,o,i,n,s,h,r.***

  Need to look at digrams or pairs of letter,

  e.g, the most common digram is "***th***"



Letter	Frequency	Letter	Frequency
e	12.7020%	m	2.4060%
t	9.0560%	w	2.3600%
a	8.1670%	f	2.2280%
o	7.5070%	g	2.0150%
i	6.9660%	y	1.9740%
n	6.7490%	p	1.9290%
s	6.3270%	b	1.4920%
h	6.0940%	v	0.9780%
r	5.9870%	k	0.7720%
d	4.2530%	j	0.1530%
l	4.0250%	x	0.1500%
c	2.7820%	q	0.0950%
u	2.7580%	z	0.0740%

Substitution Ciphers: Permutation

Attack Example:

ciphertext:

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
```

P 13.33%	Z 11.67%	S 8.33%	U 8.33%	O 7.50%	M 6.67%	H 5.83%	D 5.00%	E 5.00%
V 4.17%	X 4.17%	F 3.33%	W 3.33%	Q 2.50%	T 2.50%	A 1.67%	B 1.67%	G 1.67%
Y 1.67%	I 0.83%	J 0.83%	C 0.00%	K 0.00%	L 0.00%	N 0.00%	R 0.00%	

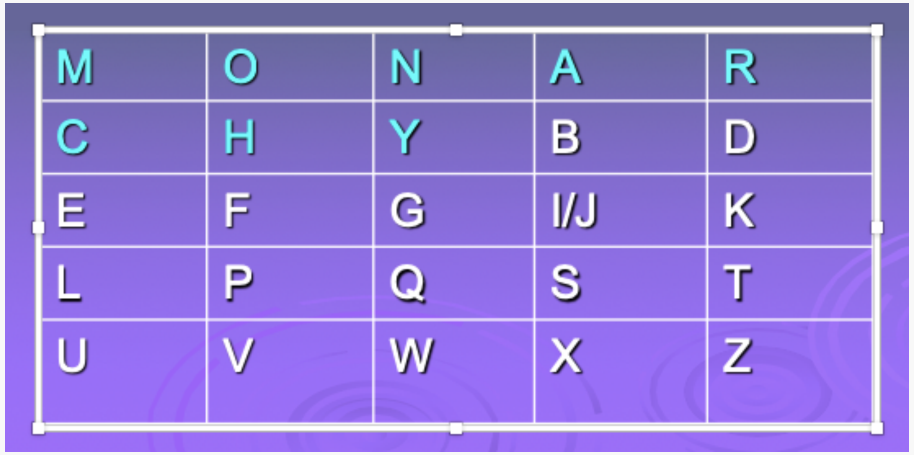
Guess P and Z are **e** and **t**; then guess ZW is **th** hence ZWP is **the;**
Proceeding with trial and error finally get:

```
it was disclosed yesterday that several informal but
direct contacts have been made with political
representatives of the viet cong in moscow
```

Substitution Ciphers: Playfair Cipher

- To lessen the extent the structure of the plaintext survives in the ciphertext:
  - Encrypt multiple letters of plaintext
  - Use multiple cipher alphabets

- The best-known multiple encryption cipher is the Playfair:
  - a 5X5 matrix of letters based on a keyword
  - fill in letters of keyword (sans duplicates)
  - fill rest of matrix with other letters
  - eg. using the keyword MONARCHY



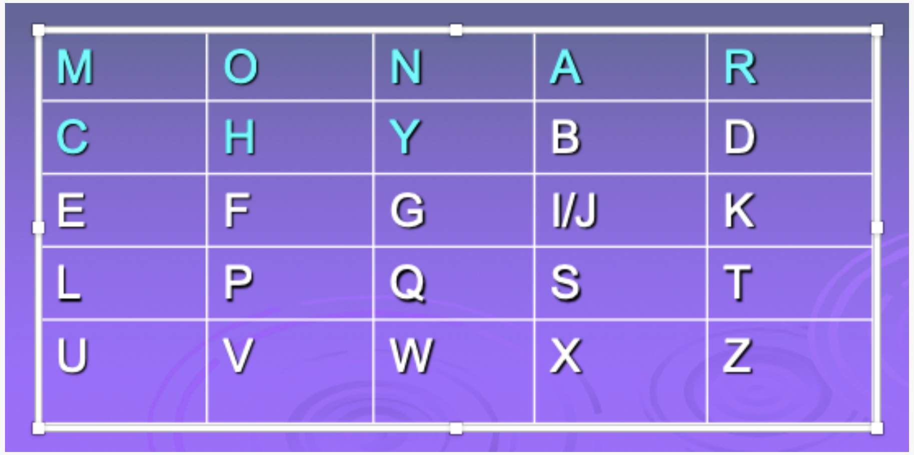
M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

Substitution Ciphers: Playfair Cipher

plaintext is encrypted two letters at a time

1. if a pair is a repeated letter, insert filler like ‘X’, balloon ->ba lx lo on
2. if both letters fall in the same row, replace each with letter to right (with the first element of the row circularly following the last) , ar->RM
3. if both letters fall in the same column, replace each with the letter below it (with the top element of the column circularly following the last), mu->CM
4. otherwise each letter is replaced by the letter in the same row and in the column of the other letter of the pair,

   hs->BP, ea->IM(JM)



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

Substitution Ciphers: One-Time Pads

- An unbreakable cryptosystem
- The key is a random sequence of 0s and 1s of the same length as the message
- Once a key is used, it is discarded and never used again
- Encryption is using XOR, bit by bit.

$$\begin{array}{rl} \text{(plaintext)} & 0\ 0\ 1\ 0\ 1\ 0\ 0\ 1 \\ \text{(key)}\ + & \underline{1\ 0\ 1\ 0\ 1\ 1\ 0\ 0} \\ \text{(ciphertext)} & 1\ 0\ 0\ 0\ 0\ 1\ 0\ 1 \end{array}$$

- Decryption uses the same key.

- Disadvantage: requires very long key and expensive to produce and transmit

Block Cipher

Block cipher: convert block of plaintext to block of ciphertext.

Hill Cipher:

Encryption: Choose an integer n, for example n=3. The key is an n*n matrix M whose entries are integers mod 26. For example, let

$$M = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix}$$

The message is written as a series of row vectors. If the message is ***abc***, we change this to the single row vector (0,1,2)

$$(0,1,2)\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix} \equiv (0,23,22)\ (mod\ 26)$$

Therefore, the ciphertext is ***AXW***.

Decryption: Find inverse of M, such that $MN \equiv I(\text{mod } 26)$, and then multiplying ciphertext to N.

Transposition cipher

A different kind of mapping

*Example of **rail fence:***

Message: ”meet me after the toga party”, write to

m e m a t r h t g p r y

e t e f e t e o a a t

The encrypted message is: MEMATRHTGPRYETEFETEOAAT

- There are more complex scheme, e.g write message in a rectangle, or reencrypted, etc.
- It make same letter frequencies as the original plaintext
- The digram and trigram frequency table can be useful

Rotor Machine

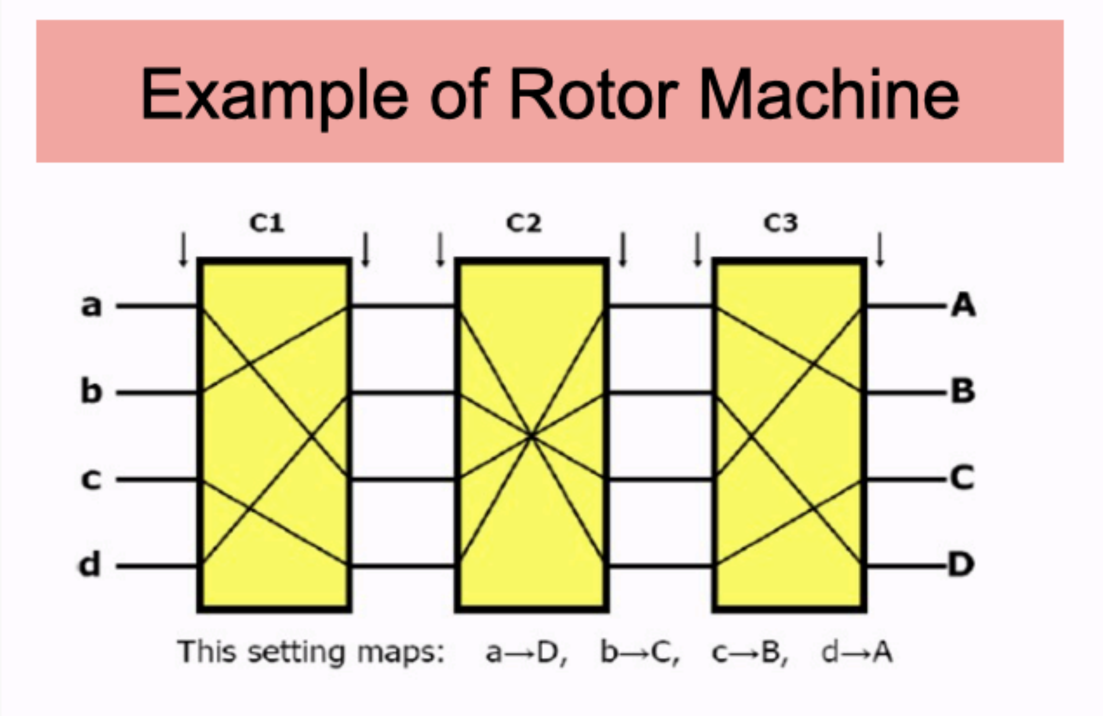
- Combine Substitution and Transposition methods.
- Mechanical encryption devices known as rotor machines were developed in WW II: Germans “Enigma” and Japanese “Purple”.
- A group of three Polish cryptologists, Marian Rejewski, Henryk Zygalski, and Jerzy Rozycki, succeeded in breaking early version of Enigma during the 1930s, and British (Alan Turing) extended the Polish techniques and successfully decrypted German messages in WW II.

Rotor Machine

Simplified Example:

- Consists a set of independently rotating cylinders
- Each cylinder has 4 input pins and 4 output pins
- Internal wiring that connects each input pin to a unique output pin
- The power of the rotor machine is in the use of multiple cylinders.

- 4*4*4 = 64 different substitutions



Example of Rotor Machine

This setting maps: a→D, b→C, c→B, d→A

Rotor Machine: Enigma

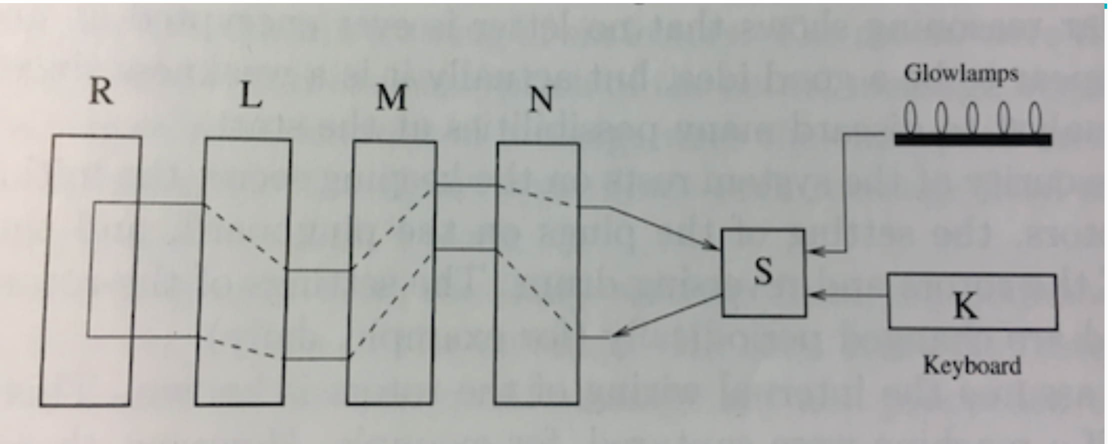


Figure 2.2: A Schematic Diagram of the Enigma Machine.

- L,M,N are rotors. One of each are 26 fixed electrical contacts, arranged in a circle
- R is the reversing drum
- K is the keyboard
- S is the plugboard

› Security of the system rests on the keeping secret the initial settings of the rotors, the setting of the plugs on the plugboard, and the internal wiring of the rotors and reversing drum.

› $6 * 26^3 = 105456$ possible initial settings

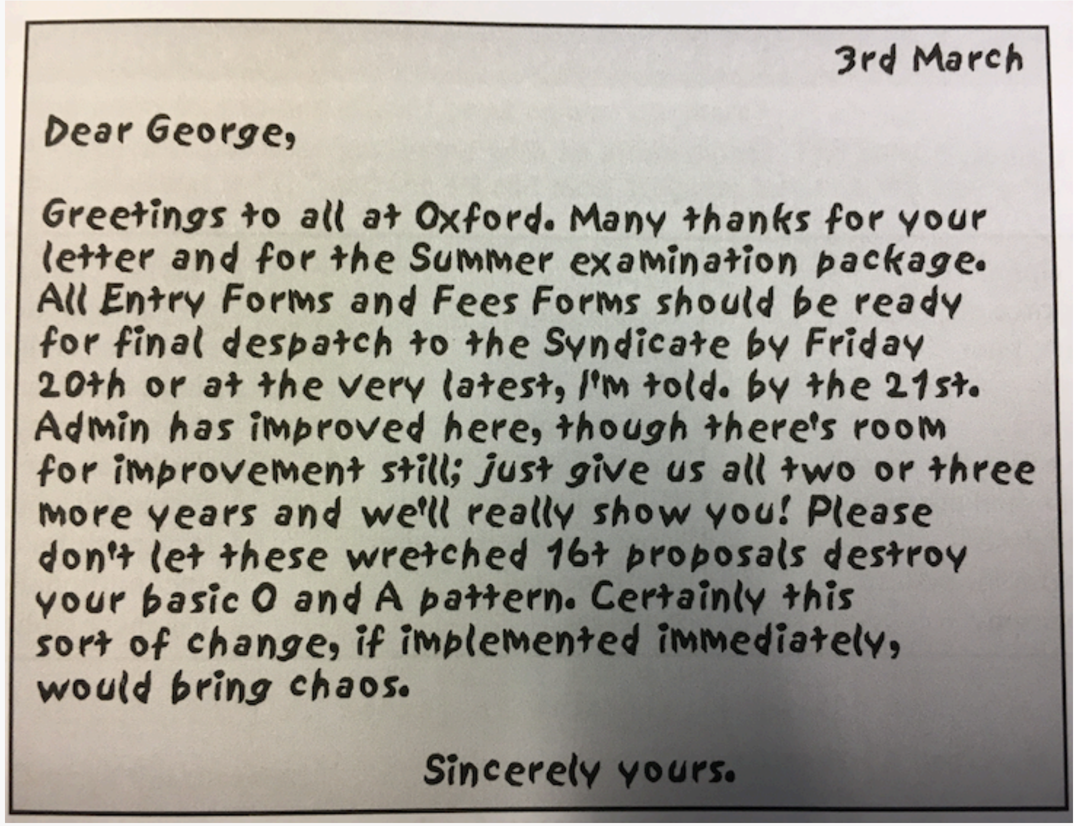
› Too many possible initializations of the machine to break the system.

› Techniques such as frequency analysis fail since the rotations of the rotors changes the substitution for each character of the message.

Steganography

- Another technique rather than encryption, **steganography**
- **“secret writing”**
- An arrangement of words or letters within an apparently innocuous text spells out of message

- A Puzzle for Inspector Morse



3rd March

Dear George,

Greetings to all at Oxford. Many thanks for your letter and for the Summer examination package. All Entry Forms and Fees Forms should be ready for final despatch to the Syndicate by Friday 20th or at the very latest, I'm told. by the 21st. Admin has improved here, though there's room for improvement still; just give us all two or three more years and we'll really show you! Please don't let these wretched 16+ proposals destroy your basic O and A pattern. Certainly this sort of change, if implemented immediately, would bring chaos.

Sincerely yours.

Exercises

- Caesar wants to arrange a secret meeting with Marc Antony, either at the Tiber (the river) or at the Coliseum (the arena). He sends the ciphertext EVIRE. However, Antony does not know the key, so he tries all possibilities. Where will he meet Caesar? (this is a tricky one)
- https://www.dcode.fr/tools-list

Thank you for your attention!