CT437 COMPUTER SECURITY AND FORENSIC COMPUTING

HISTORY OF CRYPTOGRAPHY
CRYPTOGRAPHIC CONCEPTS

Dr. Michael Schukat

OLLSCOIL NA GAILLIMHE
UNIVERSITY OF GALWAY

Lecture Outline and Motivation

- Recap: Technologies used to ensure confidentiality:
  - **Encryption (obviously)**
  - Access Control (e.g. multi-factor authentication)
  - Secure network protocols
- Therefore, this lecture provides:
  - A summary of terms linked to cryptography
  - An overview of historic cryptographic algorithms (recap CT255)
  - Some context for the next topic, **modern cryptography**

PASSWORD
MULTIFACTOR AUTHENTICATION
******
LOGGED IN
NIST National Institute of Standards and Technology U.S. Department of Commerce
www.nist.gov

Basic Terminology

- Cryptography
  - The art of encompassing the principles and methods of transforming an intelligible message into one that is unintelligible, and then retransforming that message back to its original form
    - Intelligible means “able to be understood” or comprehensible

Basic Terminology

- Plaintext
  - The original intelligible message, e.g. “THIS IS A SECRET MESSAGE”
- Ciphertext
  - The transformed message, e.g. “XPHDSYUEGSD68G4AS8AG56”
- Cipher
  - An algorithm for transforming an intelligible message into one that is unintelligible
- Key
  - Some critical information used by the cipher, known only to the sender & receiver
  - Selected from a **keyspace** K (i.e., a set of all possible keys)

Basic Terminology

- Encipher (encode)
  - The process of converting plaintext to ciphertext using a cipher and a key
- Encryption
  - The mathematical function $E_K()$ mapping plaintext P to ciphertext using the specified key K:

$$C = E_K(P)$$

Basic Terminology

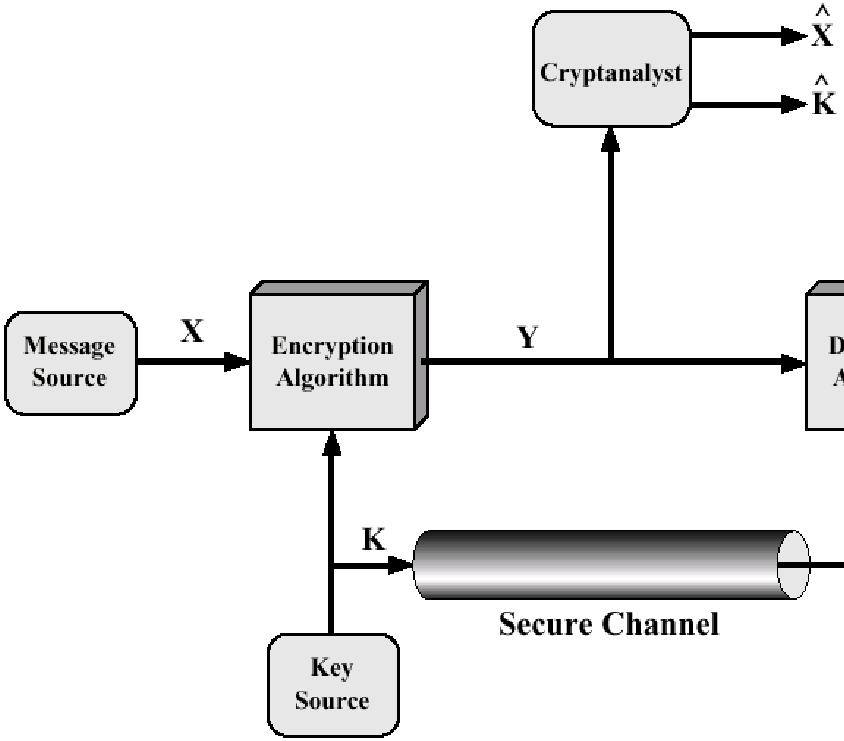
- Decipher (decode)
  - The process of converting ciphertext back into plaintext using a cipher and a key
- Decryption:
  - The mathematical function $E_K^{-1}()$ mapping ciphertext C to plaintext P using the specified key K:

    $$P = E_K^{-1}(C)$$

Basic Terminology

- Cryptanalysis
  - The study of principles and methods of transforming an unintelligible message back into an intelligible message without knowledge of the key
- Cryptology
  - The field encompassing both cryptography and cryptanalysis

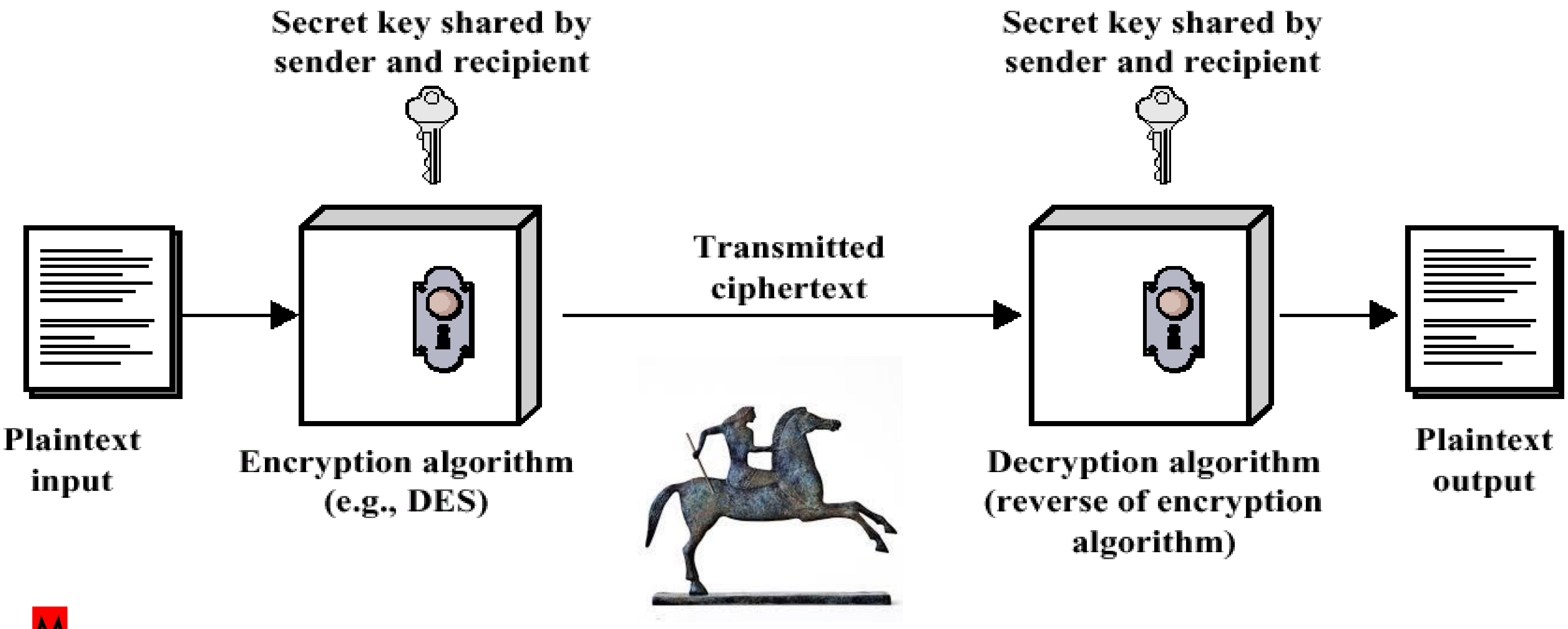
Model of Conventional Cryptosystem



$$Y = E_K(X),\ X = E_K^{-1}(Y)$$

Classical Cryptography

- Ancient ciphers have been in use for over 5,000 years
- Already used by ancient Egyptians, Hebrews and Greeks
- Normally they would follow the following scheme:


Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Caesar Cipher

- 2000 years ago, Julius Caesar used a simple substitution cipher, now known as the Caesar cipher
- First attested use in military affairs (Gallic Wars)
- Replace each letter by 3rd letter on, e.g.

  L FDPH L VDZ L FRQTXHUHG ->
  I CAME I SAW I CONQUERED

- We can describe this mapping (or translation alphabet) as:

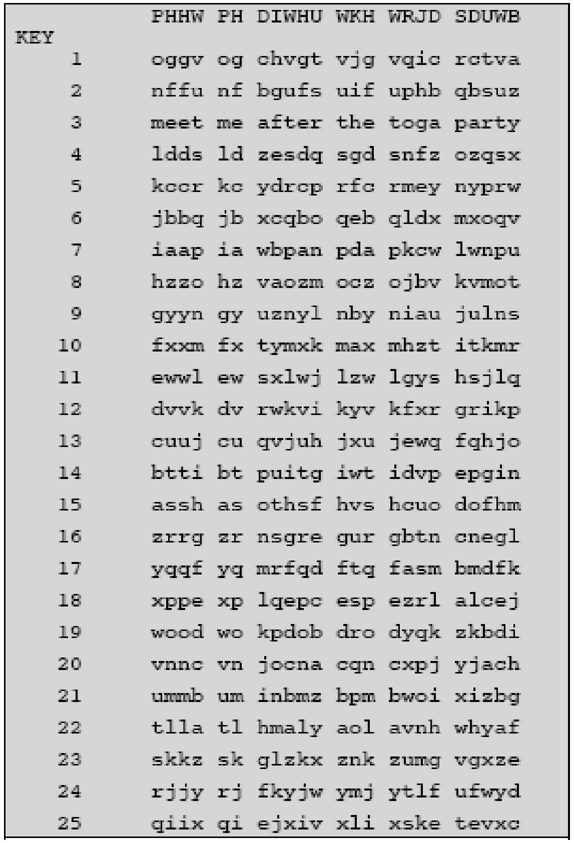
  Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ
  Cipher: DEFGHIJKLMNOPQRSTUVWXYZABC

Generalised Caesar Cipher

- More generally can use any shift from 1 to 25, i.e. replace each letter of message by a letter a fixed distance away
- Specify key letter as the letter a plaintext A maps to,
  - e.g. a key letter of F means
    A maps to F, B to G, … Y to D, Z to E
    e.g. shift letters by 5 places
- Hence have 26 (25 useful) ciphers
- Note that with this and all other historic ciphers punctuation and spaces are ignored and all text is converted to capital letters

How to break the generalised Caesar Cipher

- Try all 25 possibilities until you recover some meaningful text



KEY	PHHW PH DIWHU WKH WRJD SDUWB
1	oggv og chvgt vjg vqic rctva
2	nffu nf bgufs uif uphb qbsuz
3	meet me after the toga party
4	ldds ld zesdq sgd snfz ozqsx
5	kccr kc ydrcp rfc rmey nyprw
6	jbbq jb xcqbo qeb qldx mxoqv
7	iaap ia wbpan pda pkcw lwnpu
8	hzzo hz vaozm ocz ojbv kvmot
9	gyyn gy uznyl nby niau julns
10	fxxm fx tymxk max mhzt itkmr
11	ewwl ew sxlwj lzw lgys hsjlq
12	dvvk dv rwkvi kyv kfxr grikp
13	cuuj cu qvjuh jxu jewq fqhjo
14	btti bt puitg iwt idvp epgin
15	assh as othsf hvs hcuo dofhm
16	zrrg zr nsgre gur gbtn cnegl
17	yqqf yq mrfqd ftq fasm bmdfk
18	xppe xp lqepc esp ezrl alcej
19	wood wo kpdob dro dyqk zkbdi
20	vnnc vn jocna cqn cxpj yjach
21	ummb um inbmz bpm bwoi xizbg
22	tlla tl hmaly aol avnh whyaf
23	skkz sk glzkx znk zumg vgxze
24	rjjy rj fkyjw ymj ytlf ufwyd
25	qiix qi ejxiv xli xske tevxc

The Mono-Alphabetic (or simple) Substitution Cipher

- In the mono-alphabetic (or simple substitution) cipher each letter of the plain text is replaced with another letter of the alphabet
- It uses a fixed key which consist of the 26 letters of a “shuffled alphabet”.
- Example:
  - Plaintext alphabet (obviously): ABCDEFGHIJKLMNOPQRSTUVWXYZ
  - Ciphertext alphabet (i.e. the key): ZEBRASCDFGHIJKLMNOPQTUVWXY
  - Plaintext message: FLEEATONCEWEAREDISCOVERED
  - Ciphertext message: SIAAZQLKBAVAZOARFPBLUAOAR
- This ciphers allows for 26! (= 4.0329146e+26) possible key combinations …
  - This is too many combinations for a brute force attack where the attacker tries every single possible key!
    - This of course assumes that the attacker can identify the correctly decoded cyphertext (e.g., a text written in English)
- **Is this cipher therefore unbreakable?**

Non-trivial Cryptanalysis Attacks Against Substitution Ciphers

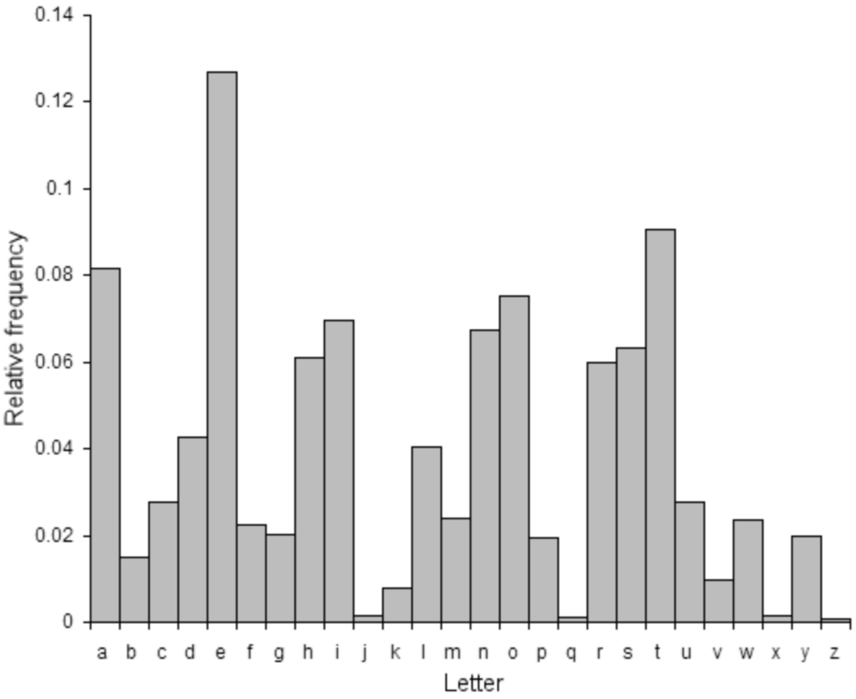
□ Frequency Analysis:
This attack relies on the fact that certain letters or symbols occur more frequently in the English language than others. By analysing the frequency of characters in the ciphertext, one can make educated guesses about the substitutions made in the cipher, ultimately revealing the plaintext
See also next slides

□ Pattern Recognition:
Cryptanalysts may also exploit patterns in the ciphertext to deduce information about the key. Recognisable patterns, such as common word endings or repeating character sequences, can provide valuable clues about the substitutions used in the cipher

□ Known-Plaintext Attack:
See next slides

Cryptanalysis via Letter Frequency Analysis

- In most written languages, letters are not equally commonly used
- For example, in the English language:
  - E is by far the most common letter followed by T,R,N,I,O,A,S
  - Other letters like Z,J,K,Q,X are fairly rare
  - See frequency table on the right
- There are tables of single, double & triple letter frequencies for all common languages
- There is an example for the cryptanalysis of a ciphertext via letter frequency analysis at the end of this slide deck



C-Program for Letter Frequency Analysis

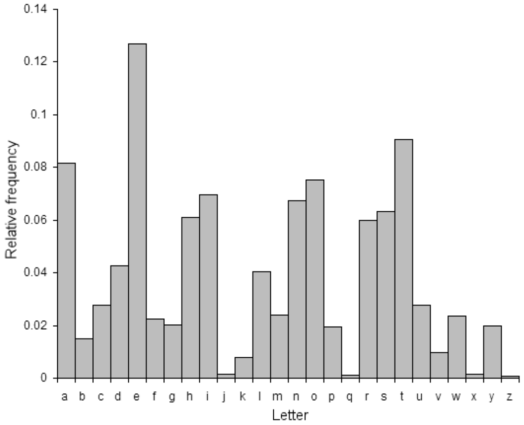
```
#include <stdio.h>
#include <string.h>
#include <ctype.h>

int main(int argc, char *argv[])
{
    FILE *fp;
    int data[26];
    char c;
    int i;

    memset(data, 0, sizeof(data));

     if (argc != 2)
       return(-1);

    if ((fp = fopen(argv[1], "r")) == NULL)
            return(-2);

    while (!feof(fp))
    {
            c = toupper(fgetc(fp));

            if ((c >= 'A') && (c <= 'Z'))
                        data[c - 65]++;
    }

    for (i = 0; i < 26; i++)
            printf("%c: %i\n", i + 65, data[i]);

    fclose(fp);
    return(1);
}
```

Known Plaintext Attacks

- The known-plaintext attack (KPA) is an attack model for cryptanalysis where the attacker has access to both
  - (some of) the plaintext (this is called a crib),
  - and its encrypted version
- See the example on the next slide

Example: Combined known-Plaintext and Pattern Recognition Attack

- You are presented with the following ciphertext which is based on a substitution cipher:
  JEPOUMJWFIFSFCVUNZIPNFJTNZDBTUMFGVMMTUPQ
- You know the original plaintext message consists of capital letters only (no spaces) and contains the following plaintext **crib**:
  MYHOMEISMYCASTLE
- How could you tackle this?

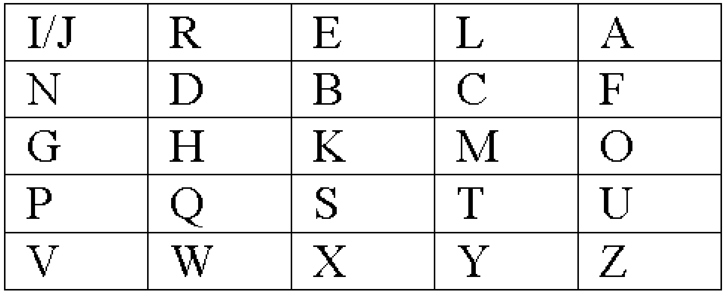


Playfair Cipher

- Not even the large number of keys in a monoalphabetic substitution cipher provides security!
- One approach to improving security was to encrypt multiple letters at once
- The **Playfair Cipher** is an example for such an approach
- Algorithm was invented by Charles Wheatstone in 1854, but named after his friend Baron Playfair

Playfair Cipher

- How it works:
  - Create a 5x5 grid of letters; insert the keyword as shown, with each letter only considered once; fill the grid with the remaining letters in alphabetic order



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

  - Letters I and J are treated the same (see example above with keyword IRELAND)
  - Letters are encrypted in pairs
  - Repeats have an X inserted:
    BALLOON -> BA LX LO ON
  - Letters that fall in the same row are each replaced with the letter on the right (OK becomes GM)
  - Letters in the same column are replaced with the letter below (FO becomes OU)
  - Otherwise, each letter gets replaced by the letter in its row but in the other letters column (QM becomes TH)

Robustness of Playfair Cipher

- The algorithm' complexity was much improved over the simple monoalphabetic cipher, since we have 26 x 26 (= 676) character combinations we have to deal with
- This requires a 676-entry frequency table for analysis (versus 26 for a monoalphabetic cipher) and substantially more ciphertext for a cryptanalysis
- Therefore, it was widely used for many years, e.g., by US & British military in WW1
- However, it **can** be broken, given a few hundred letters

Example Playfair Cipher

- Consider the Playfair Cipher and the key "PRUNEJUICE"
- Encipher the following plaintext: "KENSENTMEX"
- What is the resulting ciphertext?

Vigenère Cipher

- Blaise de Vigenère is generally credited as the inventor of the "polyalphabetic substitution cipher“
  - A monoalphabetic cipher is any cipher in which the letters of the plain text are mapped to cipher text letters based on a single alphabetic key
  - A polyalphabetic substitution ciphers uses multiple substitution alphabets
- To improve security, use many monoalphabetic substitution alphabets
- Hence each letter can be replaced by many others
- Use a key to select which alphabet is used for each letter of the message
- ith letter of key specifies ith alphabet to use
- Use each alphabet in turn
- Repeat from start after end of key is reached

Example Vigenère Cipher

- Write the plaintext out and under it write the keyword repeated
- Then using each key letter in turn as a Caesar cipher key
- Encrypt the corresponding plaintext letter. Example:

Plaintext THISPROCESSCANALSOBEEXPRESSED
Keyword CIPHERCIPHERCIPHERCIPHERCIPHE
Ciphertext VPXZTIQKTZWTCVPSWFDMTETIGAHLH
In this example have the keyword "CIPHER". Hence have the following translation alphabets:
C -> CDEFGHIJKLMNOPQRSTUVWXYZAB
I -> IJKLMNOPQRSTUVWXYZABCDEFGH

... ...

ABCDEFGHIJKLMNOPQRSTUVWXYZ

to map the above plaintext letters

Example Vigenère Cipher

- Encode the plaintext “**KENSENTME**” using the Vigenère cipher and the keyword “BABA”

- Plaintext: KENSENTME
- Key: BABABABAB
- Ciphertext: MFPTGOVNG

How to break the Vigenère Cipher

- Search the ciphertext for repeated strings of letters; the longer strings you find the better
- For each occurrence of a repeated string, count how many letters are between the first letters in the string and add one
- Factor the number you got in the above computation (e.g., 2, 5 and 10 itself are factors of 10)
- Repeat this process with each repeated string you find and make a table of common factors. The most common factor is probably the length of the keyword that was used to encipher the ciphertext. Call this number 'n'
- Do a frequency count on the ciphertext, on every nth letter. You should end up with n different frequency counts
- Compare these counts to standard frequency tables to figure out how much each letter was shifted by
- Undo the shifts and read off the message!

Example Breaking the Vigenère Cipher

Key: ABCDABCDABCDABCDABCDABCDABCD (not known to attacker)
Plaintext: **CRYPTO**ISSHORTFOR**CRYPTO**GRAPHY (not known to attacker)
Ciphertext: CSASTPKVSIQUTGQUCSASTPIUAQJB

- Our search reveals to following repetition:
  CSASTP KV SIQUT GQU **CSASTP**IUAQJB

- The distance is 16, therefore the key length n is either 2, 4, 8 or 16 characters
- Do four different frequency counts on the ciphertext, i.e., on every nth letter
- Continue as shown before

In-Class Activity: Breaking Vigenère

- Consider the following ciphertext that has been encoded using a Vigenère Cipher:

DYDUXRMHTVDVNQDQNWDYDUXRMHARTJGWNQD

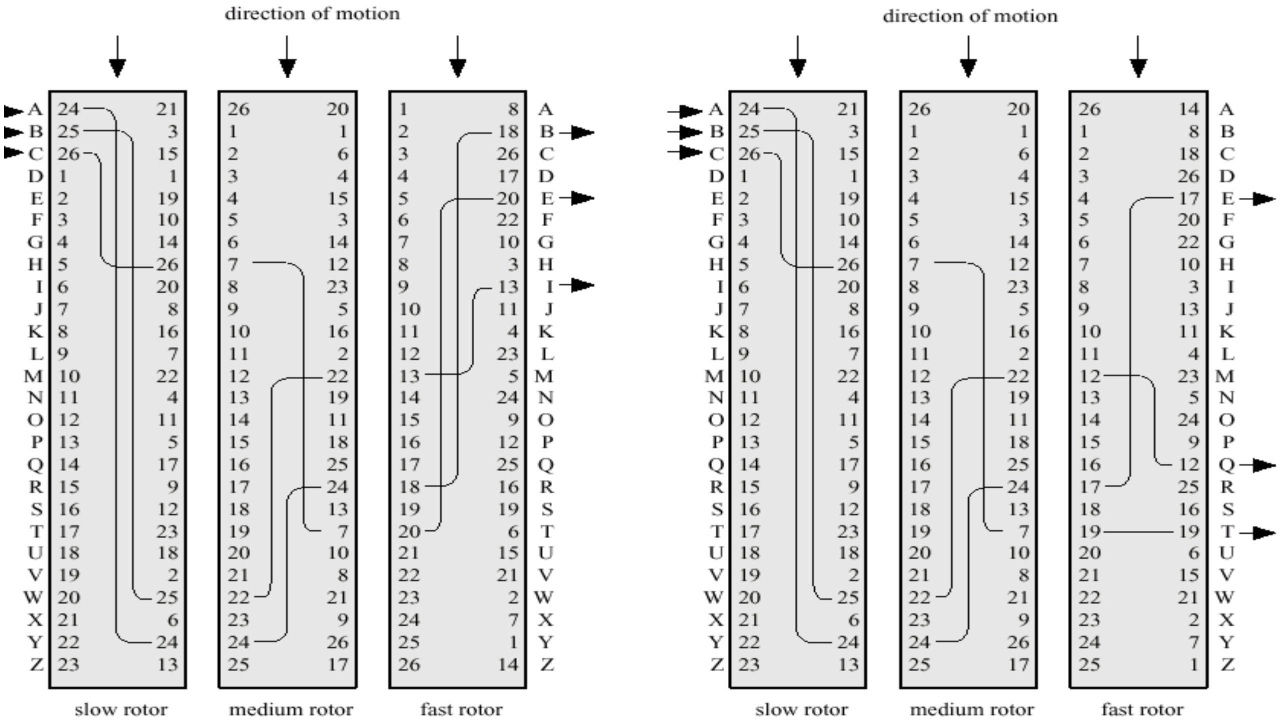
- Q1: Which repeating strings can you identify?
- Q2: What is the distance of their appearances?
- Q3: Subsequently, what is the probable key length?

Rotor Machines

- These allowed for the mechanisation / automation of message encryption and decryption and were widely used in the 20th century (until the 1970s)
- The primary components of a rotor machine are
  - a set of rotors
  - a keyboard for inputting text
  - A dashboard (e.g. array of letter-coded lamps) to show the output
- Rotors are rotating disks with an array of electrical contacts on either side
- The wiring between the contacts implements a fixed substitution of letters, replacing them in some complex fashion
- After encrypting of a letter, the rotors advance positions, changing the substitution (to be applied to the next latter that is typed in)
- By this means, a rotor machine produces a complex polyalphabetic substitution cipher, which changes with every key press

Rotor Machines

- The example below shows schematically N = 3 rotors including some of their internal wiring
- Keyboard and dashboard are not shown
- The medium rotor advances its position after a full turn of the fast rotor, and the slow rotor advances its position after a full turn of the medium rotor
- Therefore, we have a N-stage polyalphabetic substitution algorithm
- For N = 5, there are 26^N (= 11881376) steps before a substitution is repeated!



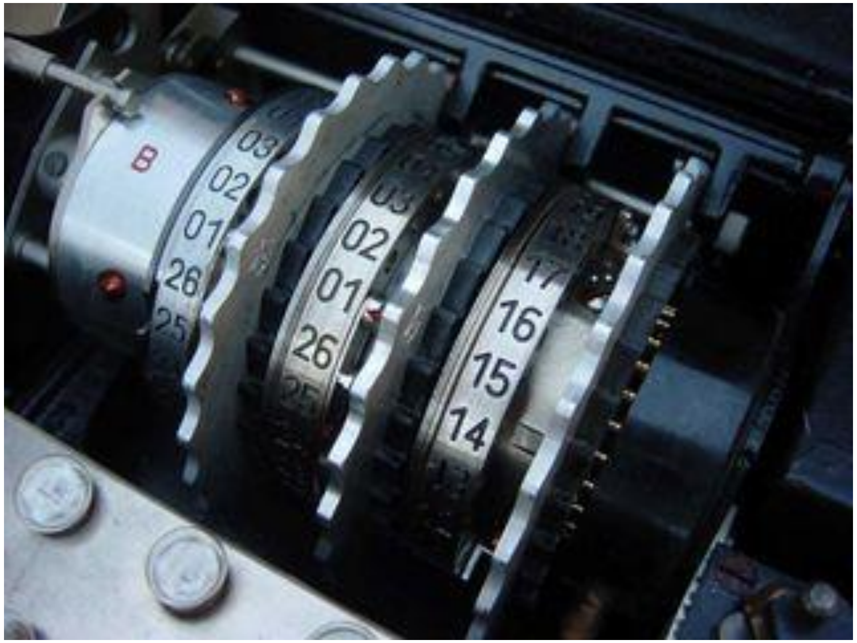
	slow rotor		medium rotor		fast rotor		
A	24	21	26	20	1	8	A
B	25	3	1	1	2	18	B
C	26	15	2	6	3	26	C
D	1	1	3	4	4	17	D
E	2	19	4	15	5	20	E
F	3	10	5	3	6	22	F
G	4	14	6	14	7	10	G
H	5	26	7	12	8	3	H
I	6	20	8	23	9	13	I
J	7	8	9	5	10	11	J
K	8	16	10	16	11	4	K
L	9	7	11	2	12	23	L
M	10	22	12	22	13	5	M
N	11	4	13	19	14	24	N
O	12	11	14	11	15	9	O
P	13	5	15	18	16	12	P
Q	14	17	16	25	17	25	Q
R	15	9	17	24	18	16	R
S	16	12	18	13	19	19	S
T	17	23	19	7	20	6	T
U	18	18	20	10	21	15	U
V	19	2	21	8	22	21	V
W	20	25	22	21	23	2	W
X	21	6	23	9	24	7	X
Y	22	24	24	26	25	1	Y
Z	23	13	25	17	26	14	Z

(a) Initial setting

	slow rotor		medium rotor		fast rotor		
A	24	21	26	20	26	14	A
B	25	3	1	1	1	8	B
C	26	15	2	6	2	18	C
D	1	1	3	4	3	26	D
E	2	19	4	15	4	17	E
F	3	10	5	3	5	20	F
G	4	14	6	14	6	22	G
H	5	26	7	12	7	10	H
I	6	20	8	23	8	3	I
J	7	8	9	5	9	13	J
K	8	16	10	16	10	11	K
L	9	7	11	2	11	4	L
M	10	22	12	22	12	23	M
N	11	4	13	19	13	5	N
O	12	11	14	11	14	24	O
P	13	5	15	18	15	9	P
Q	14	17	16	25	16	12	Q
R	15	9	17	24	17	25	R
S	16	12	18	13	18	16	S
T	17	23	19	7	19	19	T
U	18	18	20	10	20	6	U
V	19	2	21	8	21	15	V
W	20	25	22	21	22	21	W
X	21	6	23	9	23	2	X
Y	22	24	24	26	24	7	Y
Z	23	13	25	17	25	1	Z

(b) Setting after one keystroke

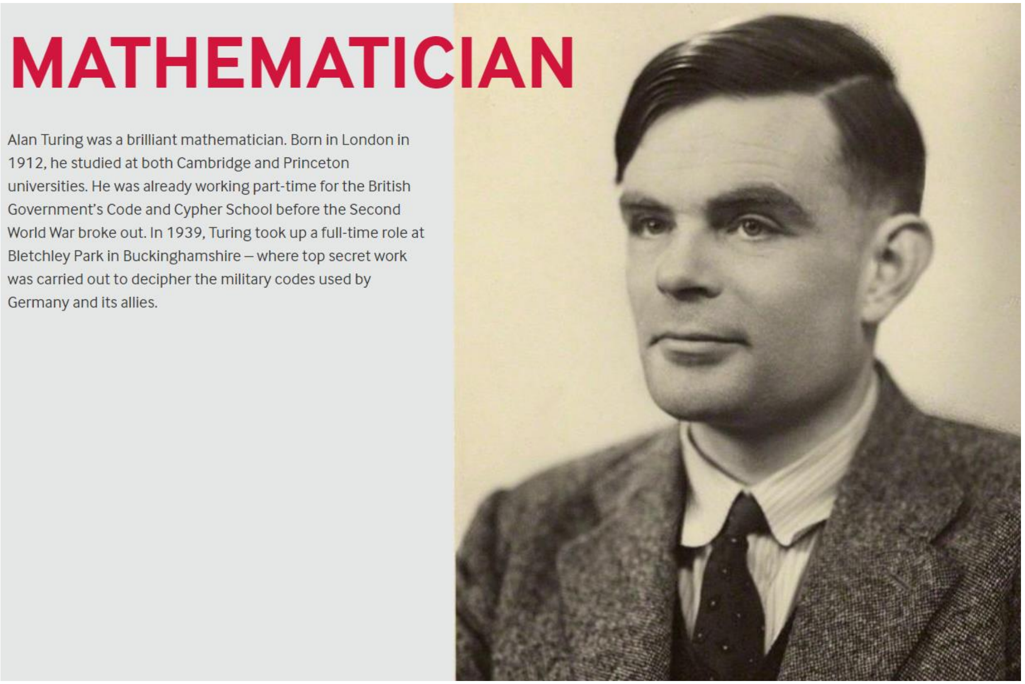
Example: The Enigma Machine



https://www.youtube.com/watch?v=-mdSvGUd0_c

How Alan Turing broke the Enigma Code

- □ https://www.iwm.org.uk/history/how-alan-turing-cracked-the-enigma-code
- □ The Imitation Game (Film, 2014)
- □ https://www.youtube.com/watch?v=nuPZUUED5uk



MATHEMATICIAN

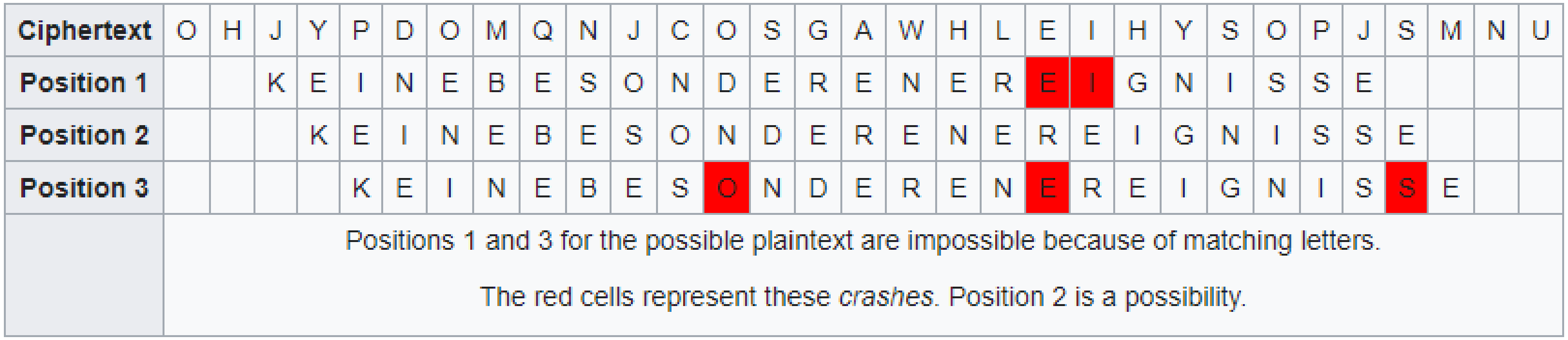
Alan Turing was a brilliant mathematician. Born in London in 1912, he studied at both Cambridge and Princeton universities. He was already working part-time for the British Government's Code and Cypher School before the Second World War broke out. In 1939, Turing took up a full-time role at Bletchley Park in Buckinghamshire – where top secret work was carried out to decipher the military codes used by Germany and its allies.

Breaking Enigma using Cribs

- Breaking Enigma was based on the following observations:
  - Plaintext messages were likely to contain certain phrases, e.g.
    - Weather reports contained the term ”WETTER VORHERSAGE”
    - Military units often sent messages containing “KEINE BESONDEREN EREIGNISSE”, i.e. “nothing to report”
  - A plaintext letter was never mapped onto the same ciphertext letter

Breaking Enigma using Cribs (Wikipedia)

- While the cryptanalysts did not know where exactly these cribs were placed in an intercepted message, they could exclude certain positions (i.e. Position 1 and 3):



Ciphertext	O	H	J	Y	P	D	O	M	Q	N	J	C	O	S	G	A	W	H	L	E	I	H	Y	S	O	P	J	S	M	N	U
Position 1			K	E	I	N	E	B	E	S	O	N	D	E	R	E	N	E	R	E	I	G	N	I	S	S	E				
Position 2				K	E	I	N	E	B	E	S	O	N	D	E	R	E	N	E	R	E	I	G	N	I	S	S	E			
Position 3					K	E	I	N	E	B	E	S	O	N	D	E	R	E	N	E	R	E	I	G	N	I	S	S	E		
	Positions 1 and 3 for the possible plaintext are impossible because of matching letters. The red cells represent these *crashes*. Position 2 is a possibility.																														

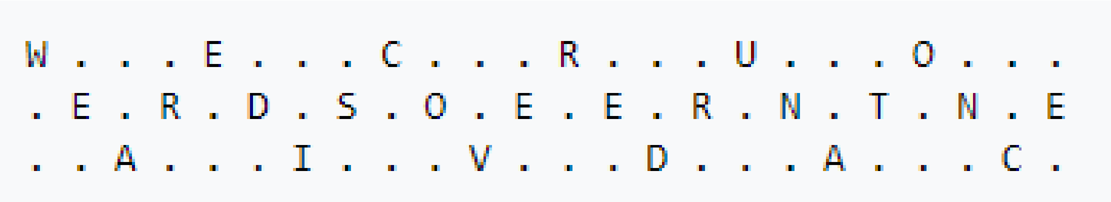
- From here on, possible rotor start positions and rotor wiring would be systematically examined using a “the bombe”, an electromechanical device designed by Alan Turing

Transposition Ciphers

- Now consider classical **transposition** or **permutation** ciphers
- These hide the message by rearranging the letter order <u>without</u> altering the actual letters used
- This can be recognised since ciphertext has the same frequency distribution as the original text

Rail Fence (Zigzag) Cipher

- Write message letters out diagonally up and down over a number of rows, then read off cipher row by row
- Example (Wikipedia): WE ARE DISCOVERED. RUN AT ONCE:



```
W . . . E . . . C . . . R . . . U . . . O . . .
. E . R . D . S . O . E . E . R . N . T . N . E
. . A . . . I . . . V . . . D . . . A . . . C .
```

- Resulting ciphertext:

```
WECRUOERDSOEERNTNEAIVDAC
```

Row Transposition Ciphers

- Write letters of message out in rows over a specified number of columns
- Then reorder the columns according to some key before reading off the columns
- Example:

Key:	4	3	1	2	5	6	7
Plaintext:	A	T	T	A	C	K	P
	O	S	T	P	O	N	E
	D	U	N	T	I	L	T
	W	O	A	M	X	Y	Z

Ciphertext: TTNA APTM TSUO AODW COIX KNLY PETZ

Note that spaces are inserted to improve readability

Combined Ciphers

- Ciphers using substitutions or transpositions are not very strong because of language characteristics
- Hence consider using several ciphers in succession to make harder:
  - two substitutions make a more complex substitution
  - two transpositions make more complex transposition
  - but a substitution followed by a transposition makes a new much harder cipher
- Similar approaches are implemented in modern ciphers

Steganography

Steganography

- An alternative to encryption
- Steganography hides the existence of a message, by:
  - Using only a subset of letters / words in a longer message marked in some way
  - Using invisible ink
  - Hiding single bits at a time in suitable computer files (e.g., images or sound files)
- Drawback:
  - Not very economical in terms of overheads to hide a message (see also examples)

Example for Steganography

- Assume an x-by-y pixel wide image is stored in RGB format
- For each pixel the colour component (R, G and B) intensity is represented by a byte
- The image can be stored in a byte array of size [x][y][3]
- For each entry we change the least significant bit to hide bitwise a message, e.g.
-
```
    R        G        B      becomes    R        G        B
01010110 11100101 10110000          01010111 11100100 10110000
11111111 10101001 00101010          11111111 10101000 00101011
11001101 10011001 11001010          11001100 10011001 11001010
...                                     ...
```
- This transformation allows the storage of the bit pattern 100101010, while causing minimal image distortions (invisible for the human eye)
- However, this method doesn't work in combination with image compression (e.g. JPEG compression)

https://stylesuxx.github.io/steganography/

Annex

1. Example cryptanalysis of a simple substitution cipher

Example Cryptanalysis of Simple Substitution Cipher

- Assume one intercepts the ciphertext below
- We know (out of the context) that
  - the plaintext message is written in English
  - The message has been encoded using the simple substitution cipher
- Intercepted ciphertext:
  UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXA
  IZVUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSXEPYE
  POPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
- We do a frequency analysis of the ciphertext and begin with the most common letters in the English language, e and t
- Guess ciphertext letters P & Z are plaintext letters e and t (we use small letters to distinguish between both):
  U**t**QSOVUOHXMO**e**VG**e**O**te**EVSG**t**WS**t**O**e**F**e**ESXUDBMETSXAI**t**V
  UE**e**H**t**HMD**t**SH**t**OWSF**e**A**ee**DTSV**e**QUZWYMXU**t**UHSXE**e**YE**e**O**e**D
  tS**t**UF**e**OMB**t**W**e**FU**et**HMDJUDTMOHMQ

Example Cryptanalysis

□ Guess (!) Z?P means *the*:

UtQSOVUOHXMOeVGeOteEVSGtWStOeFeESXUDBMET
SXAItVUEeHtHMDtSHtOWSFeAeeDTSVeQUZWYMXUtUH
SXEeYEeOeDtStUFeOMBt**W**eFUetHMDJUDTMOHMQ

□ Assume W is *h*:

UtQSOVUOHXMOeVGeOteEVSGt**h**StOeFeESXUDBMETS
XAItVUEeHtHMDtSHtO**h**SFeAeeDTSVeQUZWYMXUtUHSX
EeYEeOeDtStUFeOMBt**h**eFUetHMDJUDTMOHMQ

Example Cryptanalysis

- Guess word *that*, translating S into a:

  UtQSOVUOHXMOeVGeOteEVSG***thSt***OeFeESXUDBMET
  SXAItVUEeHtHMDtSHtOhSFeAeeDTSVeQUZWYMXUtUH
  SXEeYEeOeDtStUFeOMBtheFUetHMDJUDTMOHMQ

- Ciphertext becomes:

  UtQ**a**OVUOHXMOeVGeOteEV**a**G***that***OeFeE**a**XUDBMET
  aXAItVUEeHtHMDt**a**HtOhsFeAeeDT**a**VeQUZWYMXUtUH
  aXEeYEeOeDt**a**tUFeOMBtheFUetHMDJUDTMOHMQ

Example Cryptanalysis

- □ Guess that AeeD means *been*:
  UtQaOVUOHXMOeVGeOteEVaGthatOeFeEaXUDBMETaXAItVUEeHtHMDtaHtOhsFe**AeeD**TaVeQUZWYMXUtUHaXEeYEeOeDtatUFeOMBtheFUetHMDJUDTMOHMQ
- □ Resulting in (with A→b and D→n):
  UtQaOVUOHXMOeVGeOteEVaGthatOeFeEaXUnBMETaX**b**ItVUEeHtHM**n**taHtOhsFe**been**TaVeQUZWYMXUtUHaXEeYEeOe**n**tatUFeOMBtheFUetHM**n**JU**n**TMOHMQ

Example Cryptanalysis

□ Is HMntaHt meaning *contact*?

UtQaOVUOHXMOeVGeOteEVaGthatOeFeEaXUnBMET aXbItVUEeHt**HMntaHt**OhsFebeenTaVeQUZWYMXUtUH aXEeYEeOentatUFeOMBtheFUetHMnJUnTMOHMQ

□ Therefore (with H→ c and M→ o):

UtQaOVUO**c**X**o**OeVGeOteEVaGthatOeFeEaXUnBoETa XbItVUEe**ctcontact**OhaFebeenTaVeQUZWY**o**XUtU**c**aXEe YEeOentatUFeO**o**BtheFUet**co**nJUnT**o**O**co**Q

Example Cryptanalysis

- Does VUEect mean *direct*?
  UtQaOVUOcXoOeVGeOteEVaGthatOeFeEaXUnBoETaXbIt**VUEect**contactOhaFebeenTaVeQUZWYoXUtUcaXEeYEeOentatUFeOoBtheFUetconJUnToOcoQ
- Therefore (with V→ d, U → i and E→ r):
  itQaO**di**OcXoOe**d**GeOte**r**daGthatOeFe**r**aX**i**nBorTaXbIt**direct**contactOhaFebeenTadeQ**i**ZWYoX**i**t**i**caX**r**eY**r**eOentat**i**FeOoBtheF**i**etconJ**i**nToOcoQ

Example Cryptanalysis

- Does GeOterdaG mean yesterday?

  itQaOdiOcXoOed**GeOterdaG**thatOeFeraXinBorTaXbItdirectcontactOhaFebeenTadeQiZWYoXiticaXreYreOentatiFeOoBtheFietconJinToOcoQ

- Therefore (with G→ y and O → s):

  itQasdiscXosed**yesterday**thatseFeraXinBorTaXbItdirectcontactshaFebeenTadeQiZWYoXiticaXreYresentatiFesoBtheFietconJinToscoQ

Example Cryptanalysis

- Moscow calling?
  itQasdiscXosedyesterdaythatseFeraXinBorTaXbltdirectcontactshaFebeenTadeQiZWYoXiticaXreYresentatiFesoBtheFietconJin**ToscoQ**
- Therefore (with T → m and Q → w):
  it**w**asdiscXosedyesterdaythatseFeraXinBor**m**aXbltdirectcontactshaFebeen**m**ade**w**iZWYoXiticaXreYresentatiFesoBtheFietconJin**moscow**

Example Cryptanalysis

- X means *l*, F means *v*, B means *f*?

  itwas**discXosed**yesterdaythat**seFeraXinBormaX**bltdirectcontactshaFebeenmadewiZWYoXiticaXreYresentatiFesoBtheFietconJinmoscow

- Therefore:

  itwas**disclosed**yesterdaythat**severalinformal**bltdirectcontactshavebeenmadewiZWYoliticalreYresentativesofthevietconJinmoscow

Example Cryptanalysis

- I means *u*, Z means *t*, W means *h*, Y means *p*? itwasdisclosedyesterdaythatseveralinformal**bIt**directcontactshavebeenmade**wiZW**YoliticalreYresentativesofthevietconJinmoscow
- Therefore: itwasdisclosedyesterdaythatseveralinformal**but**directcontactshavebeenmade**with**politicalrepresentativesofthevietconJinmoscow

Example Cryptanalysis

- Finally: J means *g*:
  itwasdisclosedyesterdaythatseveralinformalbutdirectcontactshavebeenmadewithpoliticalrepresentativesofthe**vietconJ**inmoscow
- Therefore (with spaces added):
  it was disclosed yesterday that several informal but direct contacts have been made with political representatives of the vietcong in moscow