CT255
INTRODUCTION TO CYBERSECURITY

INTRODUCTION CRYPTOGRAPHY

Dr. Michael Schukat

OÉ Gaillimh
NUI Galway

Lecture Overview

- In this slide deck we are looking into some classical cryptographic concepts / algorithms, thereby identifying their weaknesses
- This levels the ground for our next topic, i.e. modern cryptography

Recap: What is Cybersecurity?

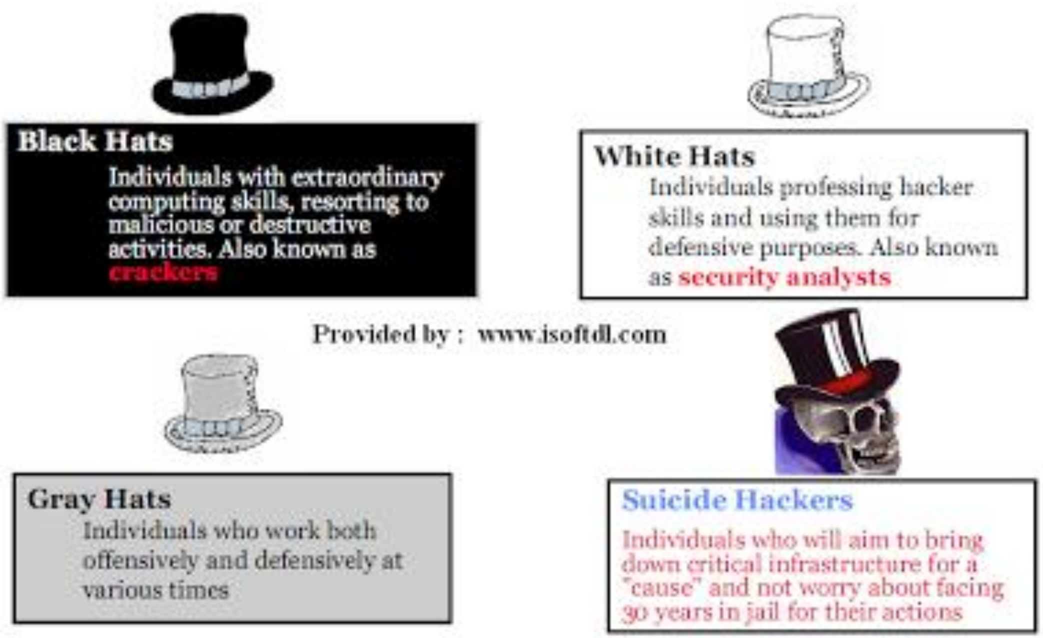
- Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes
  Source: Cisco

If this was Hogwarts…

- … the equivalent of this subject would have been taught by:

- What subject are we talking about?

Our Witches and Wizards



You find them Everywhere…

CONNACHT TRIBUNE

NEWS SPORT LIFE ENTERTAINMENT BUSINESS PROPERTY CARS

ELECTIONS

By **Bernie Ni Fhlatharta** - May 21, 2013

A Claregalway man is facing the prospect of up to 20 years in a US prison after he was named this week by the FBI as a founder member of an international internet hacking group.

[redacted] from Cloonbiggeen, Claregalway, is charged with two counts of computer hacking conspiracy – each conspiracy count carries a maximum sentence of ten years in

[redacted] is alleged by the FBI to be a member of 'LulzSec', a group of internet hackers that is a spin-off of the Anonymous hacking group. Both groups have launched numerous cyber attacks on high profile websites around the world.

[redacted] a biopharmaceutical chemistry student at NUI Galway and a past pupil of Calasanctius College, Oranmore, is listed in the FBI's court papers as being 25, however, it is understood he is only 19 or 20.

Example SQL Injections

- SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted for execution
- A way of exploiting user input and SQL Statements to compromise the database and/or retrieve sensitive data

Case Study

- Consider a SQL injection attack on an Irish online retailer revealed the following database table called "CustomerAccounts":

CustomerId	EncryptedIBAN
23	XPF7F3FD78FS8HGF9S5SL6
367	XPHDSYUEGSD68G4AS8AG56
66	XPEFGS567DS09123SD342G

- In a plaintext IBAN, The first two letters denote the country code (e.g., IE for Ireland), then two check digits, and finally a country-specific Basic Bank Account Number (BBAN), which includes the domestic bank account number, branch identifier, and potential routing information

In-Class Activity

- What are your observations / ideas regarding the entries in "EncodedIBAN“, e.g.:
  - How does the transformation work?
  - Any patterns you can see?

Some 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

Some basic Terminology

- Plaintext
  - The original intelligible message, e.g. “IE64IRCE92050112345678”
- 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)

Some 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:

$$C = E_K(P)$$

Some basic Terminology

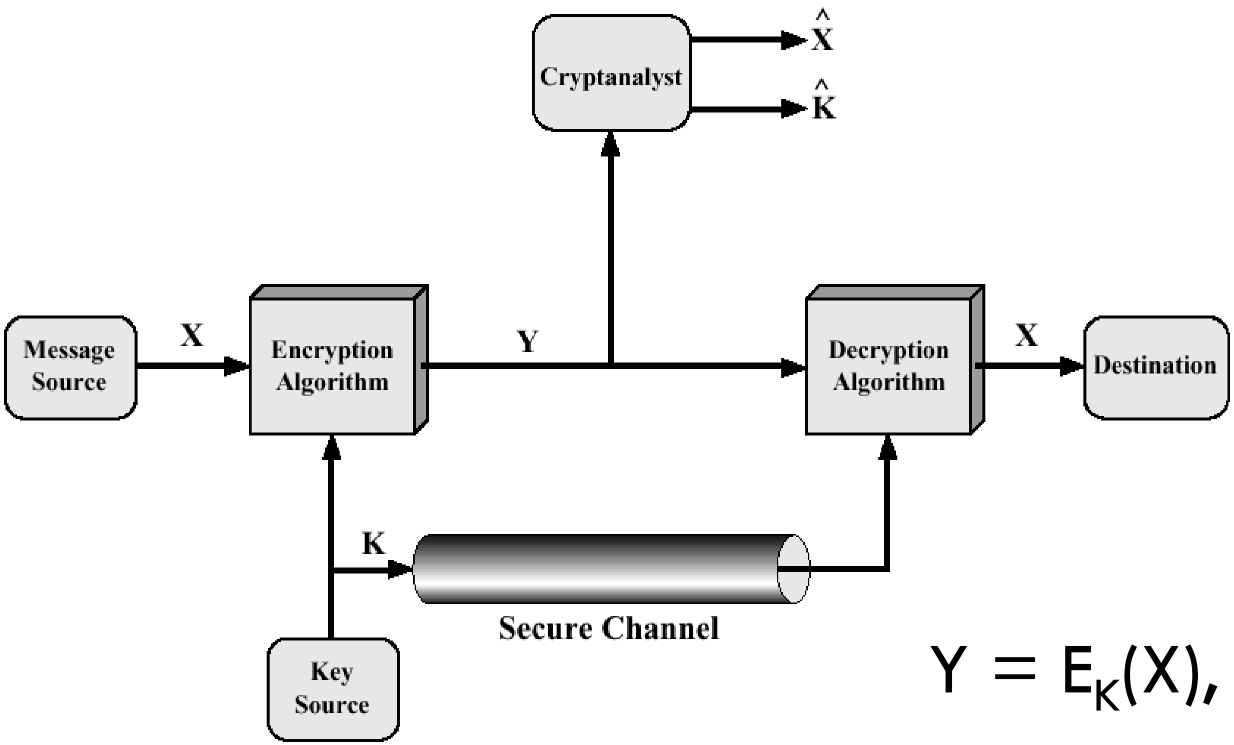
- Decipher (decode)
  - The process of converting ciphertext back into plaintext using a cipher and a key
- Decryption:
  - The mathematical function $E_K^{-1}()$ mapping ciphertext C to plaintext P using the specified key K:

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

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

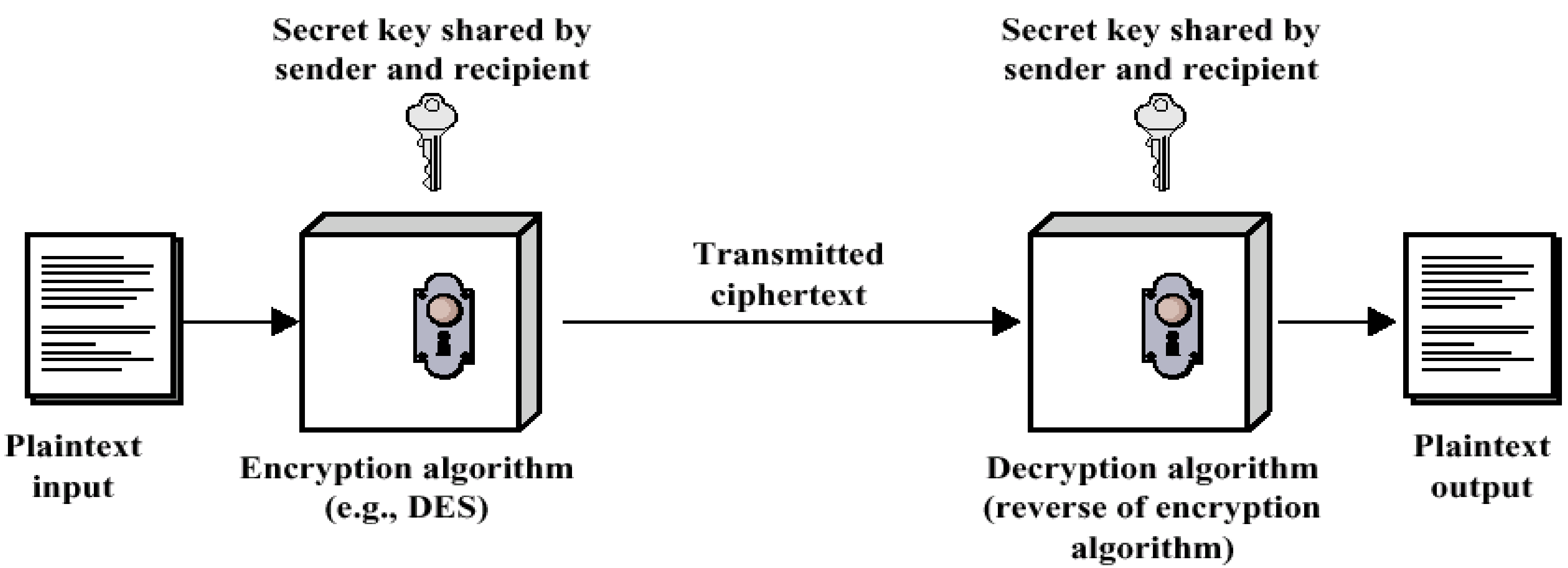
Model of Conventional Cryptosystem



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

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:



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

- 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

In-Class Activity

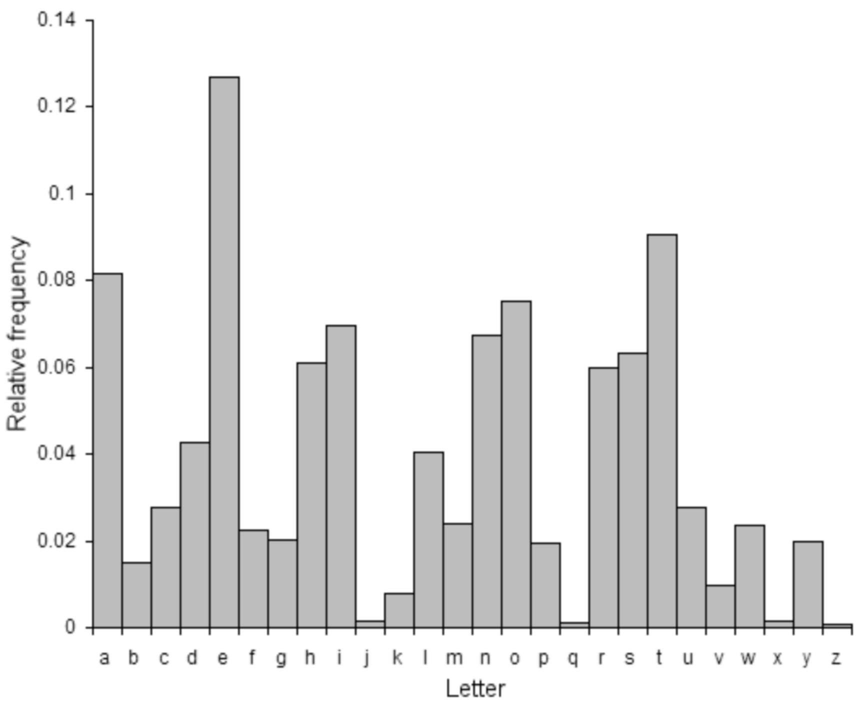
- Encode the plaintext "**KENSENTME**" using the Caesar cipher

Simple Substitution Cipher

- Cipher: Replace each plaintext letter with the corresponding ciphertext alphabet letter (only one letter at a time, therefore "simple")
- Plaintext alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ
- Ciphertext alphabet (i.e. the key): ZEBRASCDFGHIJKLMNOPQTUVWXY
- Plaintext message:
  FLEEATONCEWEAREDISCOVERED
- Ciphertext message:
  SIAAZQLKBAVAZOARFPBLUAOAR
- **26! (= 4.0329146 * 10^{26}) possible key combinations … unbreakable?**

Cryptanalysis via Letter Frequency Distribution in English Language

- Human languages are redundant
- Letters are not equally commonly used
- 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
  - certain letter combinations, e.g. TH, are quite common
- There are tables of single, double & triple letter frequencies for various languages
- See the example code on the next slide



C-Program for Frequency Analysis of single Characters

```
#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);
}
```

Example Cryptanalysis of Simple Substitution Cipher

- Given ciphertext:
  UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDB
  METSXAIZVUEPHZHMDZSHZOWSFPAPPDTSVPQUZWY
  MXUZUHSXEPYEPOPDZSZUFPOMBZWPFUPZHMDJUDT
  MOHMQ
- Count number of occurrences of each letter in text
- Guess ciphertext letters P & Z are plaintext letters e and t (we use small letters to distinguish between both):
  UtQSOVUOHXMOeVGeOteEVSGtWStOeFeESXUDBME
  TSXAItVUEeHtHMDtSHtOWSFeAeeDTSVeQUZWYMXUt
  UHSXEeYEeOeDtStUFeOMBtWeFUetHMDJUDTMOHMQ

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*:
  UtQaOVUOHXMOeVGeOteEVaGthatOeFeEaXUDBM ETaXAltVUEeHtHMDtaHtOhsFe**<u>AeeD</u>**TaVeQUZWYMXU tUHaXEeYEeOeDtatUFeOMBtheFUetHMDJUDTMOHM Q
- Resulting in (with A→b and D→n):
  UtQaOVUOHXMOeVGeOteEVaGthatOeFeEaXUnBM ETaX**<u>b</u>**ltVUEeHtHM**<u>n</u>**taHtOhsFe**<u>been</u>**TaVeQUZWYMXUt UHaXEeYEeOe**<u>n</u>**tatUFeOMBtheFUetHM**<u>n</u>**JU**<u>n</u>**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**ct****contact**OhaFebeenTaVeQUZWY**o**XUtU**c**aXEe
  YEeOentatUFeO**o**BtheFUet**co**nJUnT**o**O**co**Q

Example Cryptanalysis

- Does VUEect mean *direct*?
  UtQaOVUOcXoOeVGeOteEVaGthatOeFeEaXUnBoETaX
  bIt**VUEect**contactOhaFebeenTaVeQUZWYoXUtUcaXEeY
  EeOentatUFeOoBtheFUetconJUnToOcoQ
- Therefore (with V→ d, U → i and E→ r):
  itQaO**di**OcXoOe**d**GeOterdaGthatOeFeraXinBorTaXbIt
  directcontactOhaFebeenTadeQiZWYoXiticaXreYreOent
  atiFeOoBtheFietconJinToOcoQ

Example Cryptanalysis

- Does GeOterdaG mean yesterday?
  itQaOdiOcXoOed**<u>GeOterdaG</u>**thatOeFeraXinBorTaXbIt directcontactOhaFebeenTadeQiZWYoXiticaXreYreOent atiFeOoBtheFietconJinToOcoQ
- Therefore (with G→ y and O → s):
  itQa**<u>s</u>**di**<u>s</u>**cXo**<u>s</u>**ed**<u>yesterday</u>**that**<u>s</u>**eFeraXinBorTaXbItdirect contactshaFebeenTadeQiZWYoXiticaXreYre**<u>s</u>**entatiFeso BtheFietconJinToscoQ

Example Cryptanalysis

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

Example Cryptanalysis

- X means *l*, F means *v*, B means *f*?
  itwas**discXosed**yesterdaythat**seFeraXinBormaX**bltdir
  ectcontactshaFebeenmadewiZWYoXiticaXreYresentati
  FesoBtheFietconJinmoscow
- Therefore:
  itwas**disclosed**yesterdaythat**severalinformal**bltdirectc
  ontactshavebeenmadewiZWYoliticalreYresentativesoft
  hevietconJinmoscow

Example Cryptanalysis

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

Example Cryptanalysis

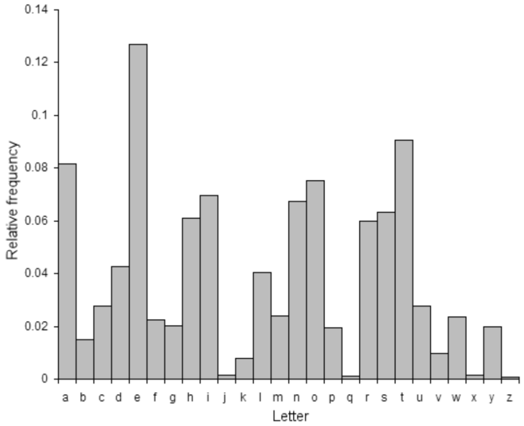
- Finally: J means *g*:
  itwasdisclosedyesterdaythatseveralinformalbutdirectcontactshavebeenmadewithpoliticalrepresentativesofthe**vietconJ**inmoscow
- Therefore (with spaces added):
  it was disclosed yesterday that several informal but direct contacts have been made with political representatives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

Known Plaintext Attacks (KPA)

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

In-Class Activity

- You are presented with the following ciphertext which is based on a simple 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 cipher provides security!
  - 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
- One approach to improving security was to encrypt multiple letters
- 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
  - 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)
- But again … Playfair can be cracked through frequency analysis of letter pairs

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

Security of Playfair Cipher

- Security much improved over simple monoalphabetic cipher, since we have 26 x 26 = 676 combinations
- This requires a 676 entry frequency table to analyse (verses 26 for a monoalphabetic) and correspondingly more ciphertext
- It was widely used for many years, e.g. by US & British military in WW1
- But it **can** be broken via frequency analysis of pairs of letters, given a few hundred letters

M

In-Class Activity

- 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
- i^{th} letter of key specifies i^{th} alphabet to use
- Use each alphabet in turn
- Repeat from start after end of key is reached

Vigenère Example

- 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

In-Class Activity (Menti)

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

How to crack 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

Key: ABCDAB CD ABCDA BCD ABCDABCDABCD

Plaintext: **CRYPTO** IS SHORT FOR **CRYPTO**GRAPHY

Ciphertext: **CSASTP** KV SIQUT GQU **CSASTP**IUAQJB

Distance is 16, therefore the key length is either 2, 4, 8 or 16 characters

In-Class Activity

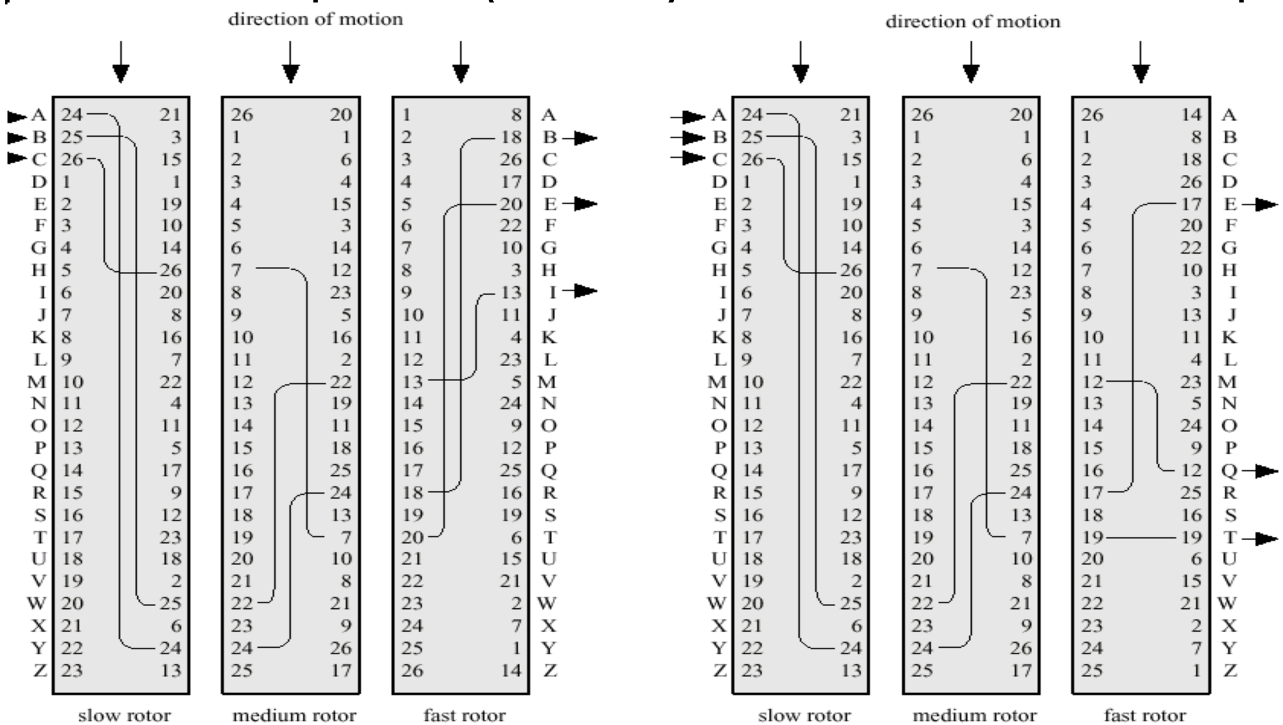
- Consider the following ciphertext that has been encoded using a Vigenère Cipher:

DYDUXRMHTVDVNQDQNWDYDUXRMHARTJGWNQD

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

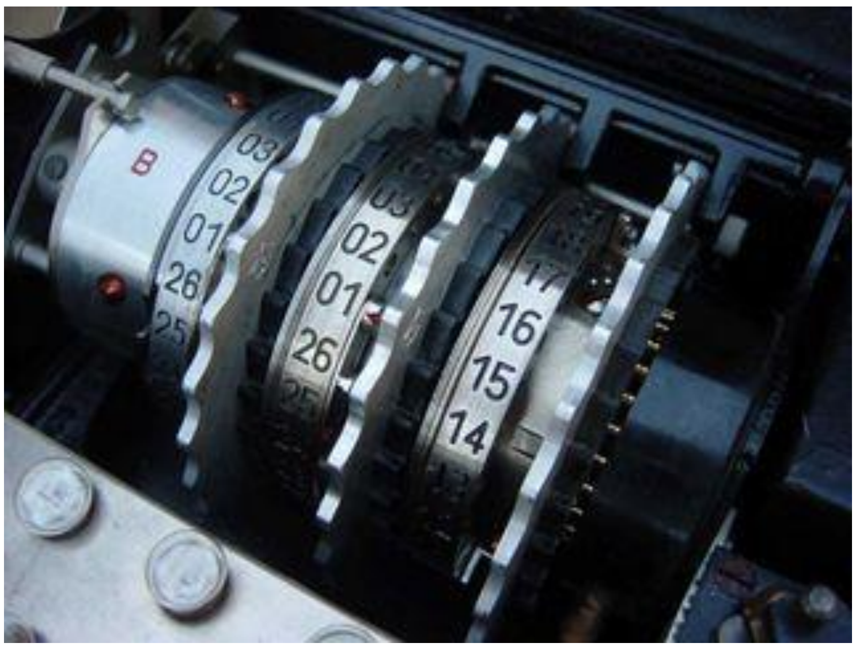
Rotor Ciphers

- The mechanisation / automation of encryption
- A N-stage polyalphabetic substitution algorithm modulo 26.
- 26^N steps before a repetition (N = 5 cylinders == 11881376 steps)



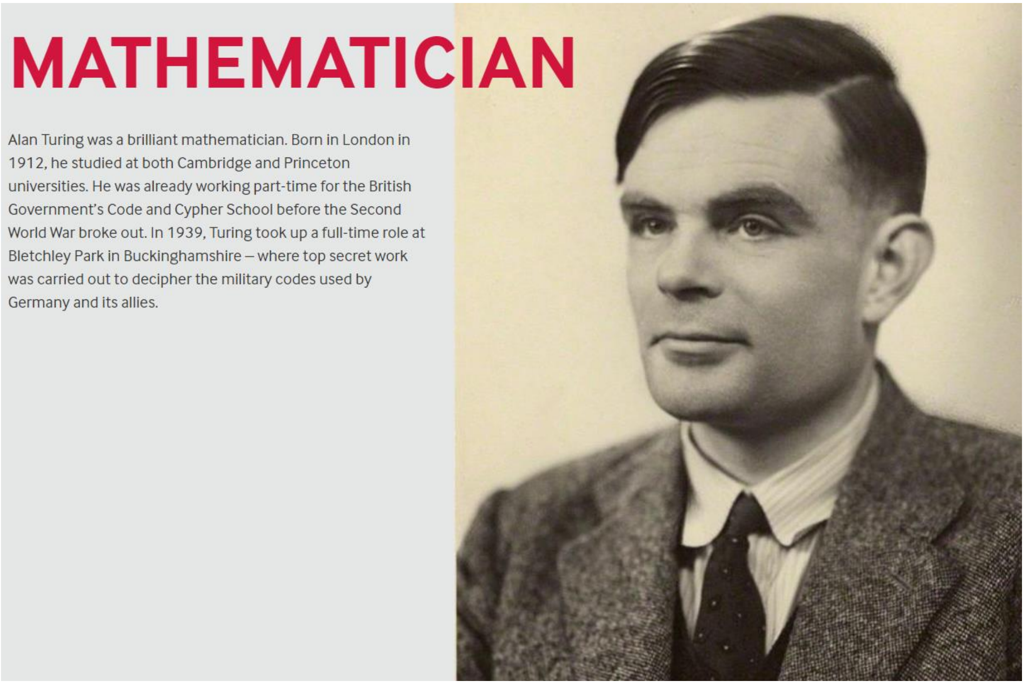
(a) Initial setting **(b) Setting after one keystroke**

The Enigma Machine



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=-mdSvGUd0_c



Breaking Enigma using Cribs

- The starting point for breaking Enigma were based on the following:
  - 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 in Bleachy Park 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 Cipher

- Write message letters out diagonally over a number of rows, then read off cipher row by row.
- Example: write message out as:

```
m e m a t r h t g p r y
 e t e f e t e o a a t
```

- Resulting ciphertext:

```
MEMATRHTGPRYETEFETEOAAT
```

In-Class Activity (Menti)

- The following ciphertext was encoded using the rail fence cipher over X rows:
  LEOREEOFEATUHPSMTELE
- Please decode

Row Transposition Ciphers

- This is a more complex transposition.
- 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 (spaces are inserted to
                                                improve readability)
```

Product Ciphers

- Ciphers using substitutions or transpositions are not secure 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
- This is bridge from classical to modern ciphers

Steganography

Steganography

- An alternative to encryption
- Hides existence of message:
  - Using only a subset of letters/words in a longer message marked in some way
  - Using invisible ink
  - Hiding in LSB in graphic image or sound file
- Drawback:
  - Not very economical in terms of overheads to hide a message (see also assignment)

(Silly) Steganography Example

Shopping List:

- LEEKS
- EGGS
- TOMATOS
- MARGERINE
- EDAMER CHEESE
- GRAPES
- ONIONS

(Silly) Steganography Example

Shopping List:

- LEEKS
- EGGS
- TOMATOS
- MARGERINE
- EDAMER CHEESE
- GRAPES
- ONIONS

Example for Steganography

- Assume an x-by-y pixels image is stored in RGB format.
- For each pixel each colour component (R, G and B) intensity is represented by a byte
- So the image can be stored in a byte array of size [x][y][3]
- For each entry we change the LSB 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 preserving the main image characteristics.
- Since only the LSB of the colour information changes, the image is only very slightly distorted.
- However, image compression (e.g. JPEG) will interfere with steganographic content!