ĐẠI HỌC TÔN ĐỨC THẮNG
TON DUC THANG UNIVERSITY

ATTACKS, SOCIAL ENGINEERING

HUYNH NGOC TU, Phd
Faculty of Information Technology

Outlines

1. Attacks, social engineering

- Phishing, pretexting, “human” properties
- A practical problem: issues in authentication

2. Historical encryption schemes...

- Prehistory of crypto - substitution ciphers
- Prehistory of crypto - transposition

Social Engineering: the art of manipulating people

Wikipedia definitions, examples...

- Pretexting: using an invented scenario to engage a targeted victim to increase the chance the victim will divulge information. An elaborate lie...

“Hello, this is Alice calling from Microsoft Security Services. We are recording a security alert with your computer..”.

- Phishing: attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity...

“Dear valued PayPal Customer, Due to a policy update we need to verify your PayPal account. Please download the attached file...”.

Social Engineering: the art of manipulating people

Examples...

336 computer science students at the University of Sydney were sent an email asking them to supply their password on the pretext that it was required to 'validate' the password database after a suspected breaking.

138 of them returned a valid password. Some were suspicious: 30 returned an invalid password. 200 changed their passwords.

Social Engineering: the art of manipulating people

Many banks/businesses train their customers to act in unsafe ways:

It's not prudent to click on links in emails, so if you want to contact your bank you should type in the URL or use a bookmark — yet bank marketing departments continue to send out emails containing clickable links. It's not prudent to give out security information over the phone to unidentified callers— yet we all get phoned by bank staff who aggressively demand security information without having any well-thought-out means of identifying themselves.

Human strengths and weaknesses

Behavioural psychology...

- Weaknesses:
  - short term memory limited to about 5 choices
  - poor recall
  - poor at operating equipment
  - risk averse: dislike losing $100 more than we like winning $100 also poor evaluation of risk - we are more worried about well-publicised things
  - Heart takes over when head runs out
  - Social psychologists point out that we do bow to “authority” - even in the face of evidence from our own eyes.
- Strengths:
  - Can recognize humans, detect subtle patterns, and understand speech

Practical security problems...

Devices, passwords, fingerprints...

- Something you have, something you know, something you

(or facetiously: something you once had, something you've forgotten, something you once were).

Most central is the password: PINs, and passwords.

Note that there may be different complexity requirements.

- For example a four digit PIN may be OK on an ATM, because the machine can lock the account after (say) three invalid guesses. By contrast an NUSNET password should be much longer, because an attacker could attack (brute force) all the 4-digit passwords in a very short time.

Password concerns

- Reliability, memorability, disclosure...

If too long, there may be problems in entering the data correctly, although grouping helps (928377461534518 versus 9283 7746 1534 5198).

If you have to remember the password, we tend to base passwords on something like our family names or interests, along with a couple of digits. Unfortunately this makes the passwords hackable - dictionary attacks using words and names and combinations. Forced changes can cause problems - for example a password “family”: secret1pass, secret2pass, secret3pass and so on.

Password concerns

Run a test, with three groups :

- self chosen password. 30% hackable, easy to remember
- Mnemonic passphrase. 10% hackable, easy to remember
- 8 characters at random. 10% hackable, hard to remember

Password phishing countermeasures

Hits and misses

- Client certificates: User has a certificate on their machine which authenticates them. Of course it could be stolen.
- Let the browser remember them.
- Soft keyboards for password entry.
- Customer education: Check the English!
- Microsoft passport.
- Browser flags Phishing sites using lists of “BAD” URLs.
- 2-factor/2-channel authentication
- Password manglers: User has a single password which is hashed (mangled) according to the web site URL.

Completely Automated Public Turing Test...

... to Tell Computers and Humans Apart (CAPTCHA)

A computer intelligence test posed by Alan Turing, where you put a computer in one room and a human in another, and invite a human to try to tell them apart.

CAPTCHA is kind of the reverse - the computer (server) attempts to tell the difference using a known hard problem:

UNIX passwords

- When you log in with your account name and password

The password is hashed and the resulting hash is compared to the hash stored in a password file. If they are equal, the system accepts that you have typed in the correct password and grants you access.

- Brute force cracking...

If the hashed password list is available, given enough time, brute force cracking will get a password. BTW - You cannot try to log in using all the possible passwords, as UNIX systems enforce 10 second timeouts after three consecutive login failures.

Dictionary cracking

- Crack software: A popular cracking utility is called Crack.
- Crack can use user-definable rules for word manipulation or mutation to maximize dictionary effectiveness: substitute numbers for certain letters, add prefixes or suffixes, or switch case or order of letters.
- Crack merges dictionaries, turns the password files into a sorted list, and generates lists of possible passwords from the merged dictionary or from information gleaned about users from the password file.

Key points/jargon

Summary:

- Social engineering, pretexting, phishing
- Password reliability, memorability.
- Mnemonic passwords.
- Client certificates, 2-factor, 2-channel authentication
- CAPTCHA
- Brute force and dictionary cracking

Julius Cæsar cipher...

- Julius Cæsar cipher…

Cæsar (rotation) cipher over Roman letters: Key is "+3".

I C L A V D I V S

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

M F O D Z G M Z X

Can define the transformation mathematically:

$c = E(k,p) = (p + k) \bmod 23$

$p = D(k,c) = (c-k) \bmod 23$

Julius Cæsar cipher...

- Cryptanalysis of rotation ciphers: In the above example - we only have 22 possible useful ciphers! So an attacker can try each in turn: a brute force search

Examples of rotation ciphers

- Union (North) and Confederate (South) ciphers

Used in the American Civil war, they can be used as simple rotation cipher. The southern one has a keyspace of 26, and a useful keyspace of only 25.

Substitution

Substitution cipher systems encode the input stream using a substitution rule. The Cæsar cipher is an example of a simple substitution cipher system.

- Random substitution - a monoalphabetic substitution cipher

Code	Encoding
A	Q
B	V
C	X
D	W
…	…

If the mapping was more randomly chosen it is called a monoalphabetic substitution cipher, and the keyspace for encoding 26 letters would be

$$26! - 1 = 403,291,461,126,605,635,583,999,999.$$

Cryptanalysis of substitution cipher

- How safe is this cipher? (Not at all!)

If we could decrypt 1,000,000 messages in a second, then the average time to find a solution by trying decryptions would be about 6,394,144,170,576 years!

We might be lulled into a sense of security by these big numbers, but of course this sort of cipher can be subject to frequency analysis... The problems are that:

1 letters are not equally common: ETAOINSHRDLU!

2 human languages have high levels of redundancy: (fr xmpl, hgh ndrsn s tchng cs2107 ths smstr).

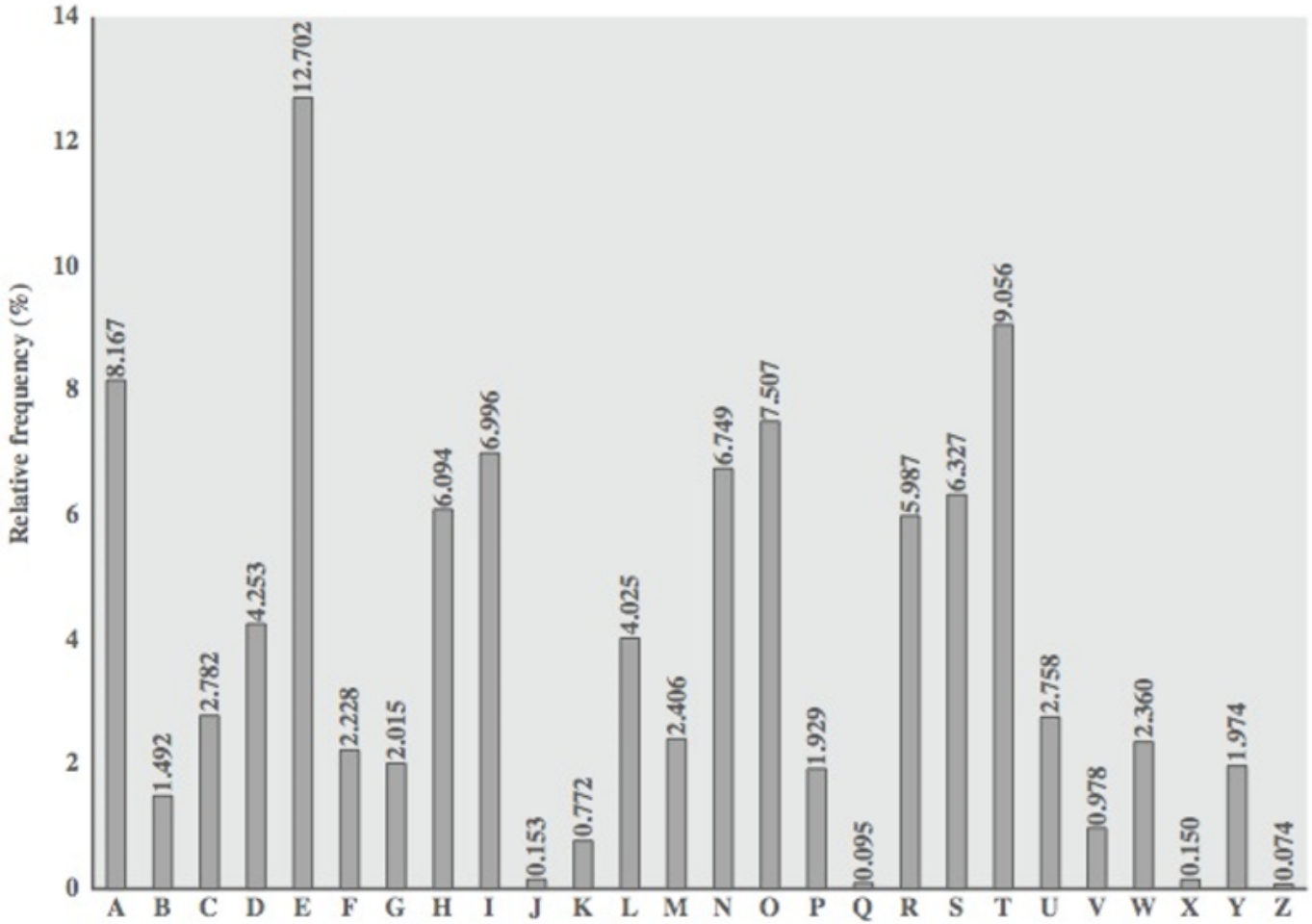
We have tables of single, double & triple letter frequencies for languages.

Cryptanalysis of mono-alphabetic ciphers

Frequencies of english text:

These ciphers do not change relative letter frequencies

- The central concept of this was discovered and described by Arabian scientists in the 9th century.
- An attacker can calculate the frequencies for ciphertext. The most common ciphertext letter might translate to an E.



Cryptanalysis of mono-alphabetic ciphers

- Example encrypted message

EV YQS CVV MIWK FRPC FRQF FRV IQFV WM
FIQSCKPCCPWS ACPSN IVJVFPFPWS RQC FW QJJIWQYR
ZVIW FW QYRPVDV KWIV QSB KWIV IVTPQXTV
FIQSCKPCCPWS. RWEVDVI EV LSWE FRQF FRV
FRVWIVFPYQT IQFV CRWATB ...

V occurs most often, F next and so on, so replace V with E...

Example - first step of decoding:

EV YQS CVV MIWK FRPC FRQF FRV IQFV WM

-E -A- -EE F-O- THI- THAT THE -ATE OF

FIQSCKPCCPWS ACPSN IVJVFPFPWS RQC FW

T-A---I--IO- --I-- -E-ETITIO- HA- TO

QJJIWQYR ZVIW FW QYRPVDV KWIV QSB KWIV

A---OA-H -E-O TO A-HIE-E -O-E A-- -O-E

Polyalphabetic ciphers

- Polyalphabetic substitution ciphers improve security:

  There are more alphabets to guess and hence a flatter frequency distribution. We use a key to select which cipher is used for each letter of message.

Polyalphabetic ciphers

Vigenère (1520) uses a tableau, and a key:

	A	B	C	D	E	F	G	H	...
A	A	B	C	D	E	F	G	H	...
B	B	C	D	E	F	G	H	I	...
C	C	D	E	F	G	H	I	J	...
D	D	E	F	G	H	I	J	K	...
E	E	F	G	H	I	J	K	L	...
F	F	G	H	I	J	K	L	M	...
G	G	H	I	J	K	L	M	N	...
H	H	I	J	K	L	M	N	O	...
...	...	...	...	...	...	...	...	...	...

Vigenère

- Keyword is BAD, so encoding HAD A FEED results in:

Key	B	A	D	B	A	D	B	A
Text	H	A	D	A	F	E	E	D
Cipher	I	A	G	B	F	H	F	D

- If we can discover the length of the repeated key (in this case 3), and the text is long enough, we can just consider the cipher text to be a group of interleaved monoalphabetic substitution ciphers and solve accordingly.

Vigenère

- Cryptanalysis of Vigenère cipher:
  - Multiple ciphertext letters for each plaintext letter, and so letter frequencies are obscured (but not totally lost) Start with letter frequencies, see if monoalphabetic or not. If not, then need to determine number of alphabets.

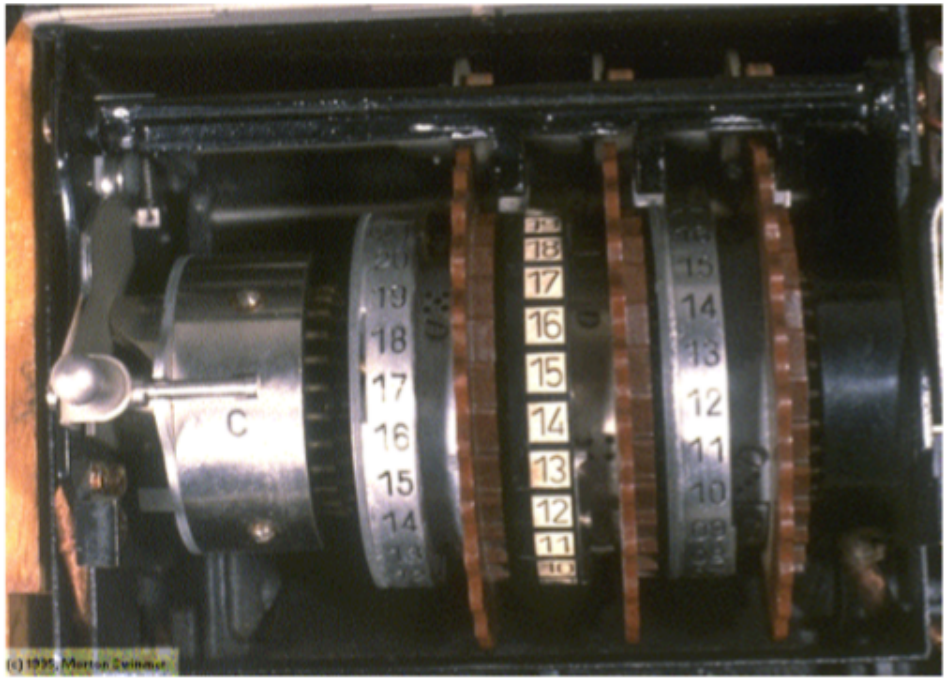
Example of a polyalphabetic substitution cipher

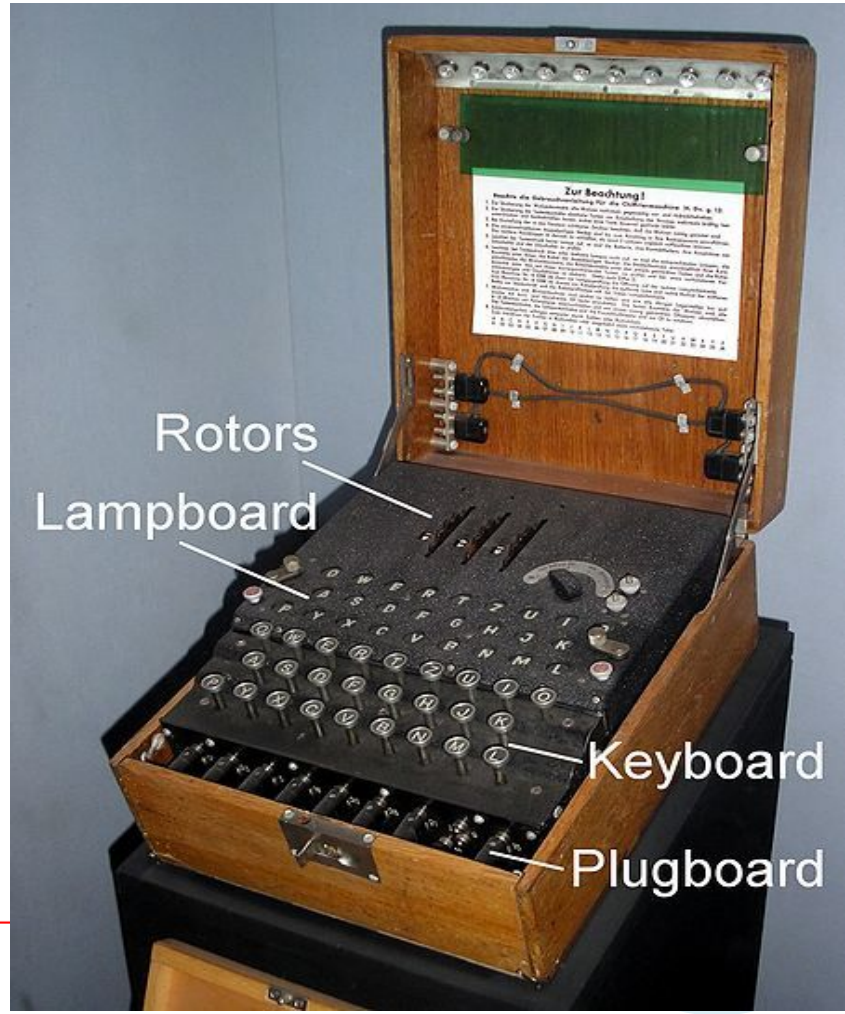
- The M-94 cipher Used by the US army from 1922 to 1942. It had 25 disks, each containing a random sequence of the letters A-Z around the outside.

Polyalphabetic substitution cipher machine...

Polyalphabetic substitution (rotor) machines: 70 years ago...

- The Enigma machine, and closeup of its rotors...

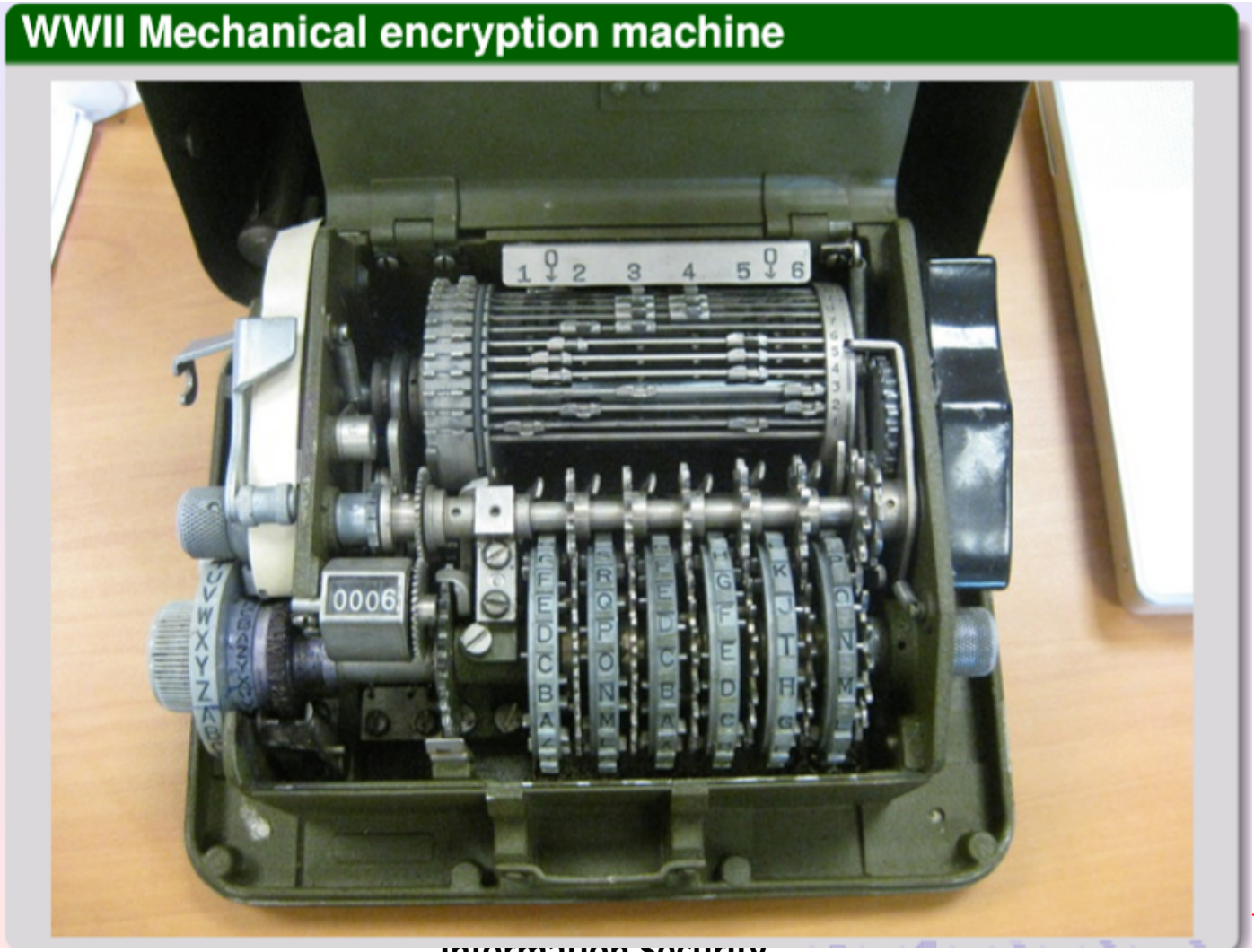




Polyalphabetic substitution cipher machine...

Dr James Grime on Enigma

US M209 Rotor machine



What is inside? A Beaufort cipher

- Reversed tableau...
- H encoded with key 5 is X.

More material at

http://yannloup.free.fr/m209simulator/bin/

	A	B	C	D	E	F	G	H	...
0	Z	Y	X	W	V	U	T	S	...
1	A	Z	Y	X	W	V	U	T	...
2	B	A	Z	Y	X	W	V	U	...
3	C	B	A	Z	Y	X	W	V	...
4	D	C	B	A	Z	Y	X	W	...
5	E	D	C	B	A	Z	Y	X	...
6	F	E	D	C	B	A	Z	Y	...
7	G	F	E	D	C	B	A	X	...
...	...	...	...	...	...	...	...	...	...

Cryptanalysis: Kasiski method

- Method developed by Babbage (1854) and Kasiski (1863):
  - Repetitions in ciphertext give clues to period so find same plaintext an exact period apart which results in the same ciphertext (of course, could also be random fluke)
  - Then attack each monoalphabetic cipher individually using same techniques as before.

Despite this - systems used into 20th century: The Zimmermann Telegram (or Zimmermann Note; German: Zimmermann-Depesche; Spanish: Telegrama Zimmermann) was a 1917 diplomatic proposal from the German Empire to Mexico to make war against the United States. The proposal was declined by Mexico, but angered Americans and led in part to the declaration of war in April [Wikipedia].

One time pad/Vernam's cipher

- An "unconditionally secure" scheme:
  - One time pad provides perfect secrecy.
  - The key is a sequence of random key letters, each letter used once only, and available at only the sender and receiver.

Playfair cipher

- Improvement over mono-alphabetic: the Playfair cipher.
  - Invented by Charles Wheatstone in 1854, named after Baron Playfair. 5X5 matrix of letters based on a keyword.
  - 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

Playfair cipher

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

Encryption: two letters at a time:

- if a pair is a repeated letter, insert filler like 'X'
- if both letters fall in the same row, replace each with letter to right (wrapping back to start from end)
- if both letters fall in the same column, replace each with the letter below it (wrapping to top from bottom)
- otherwise each letter is replaced by the letter in the same row and in the column of the other letter of the pair

Cryptanalysis of Playfair cipher

- Security improved over monoalphabetic:
  - Have 26×26 = 676 two-letter pairs (digrams), and would need a 676 entry frequency table to analyse (verses 26 for a monoalphabetic). and correspondingly more ciphertext.
  - Was widely used for many years eg. by US & British military in WW1 It can be broken, given a few hundred letters since it still has much of plaintext structure

Simple ciphers – transposition

Transposition ciphers

- Transposition ciphers just re-order the letters of the original message. This is known as an anagram:
  - parliament is an anagram of partial men
  - Eleven plus two is an anagram of Twelve plus one
  - Doctor Who is an anagram of Torchwood
- Perhaps you would like to see if you can unscramble "im a jerk but listen", or "ipod lover".

Transposition ciphers

- Transposition/permutation ciphers:
  - Hide message by rearranging letter order.
  - Have 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
eg. 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
```

giving ciphertext

```
MEMATRHTGPRYETEFETEOAAT
```

Transposition ciphers

Detecting a transposition cipher

- Detect a transposition cipher with the frequencies of the letters, and letter pairs.
- If the frequency of single letters in ciphertext is correct, but the frequencies of letter pairs is wrong, then the cipher may be a transposition.
- This sort of analysis can also assist in unscrambling a transposition ciphertext, by arranging the letters in their letter pairs.

Key points/jargon

Summary:

- Substitution ciphers
  - Cæsar/rotation,
  - Random (mono-alphabetic substitution)
  - Vigenère, Beaufort (poly-alphabetic substitution)
  - One time pad (Vernam's cipher)
  - Playfair
- Transposition/permutation ciphers
  - Rail fence cipher
- Frequency analysis for cryptanalysis