About the Speaker

IAMN OTAP ROFE SSIO NALC RYPT OGRA PHER XIAC TUAL
LYSP ENTM OSTO FMYW ORKI NGLI FEAS AMET ALLU RGIC
ALEN GINE ERBU TRET IEDI NTOT EACH INGS TOPM YINI
ERES TINT HESU BJEC TSTE MSFR OMRE ADIN GAPA PERO
NTHE MATH EMAT ICSO FPUB LICK EYCR YPTO GRAP HYIN
THES EVEN TIES THEN DELV INGB ACKI NTOT HEHI STOR
YUSE SAND ABUS ESOF THES UBJE CTX MYCU RREN TINV
OLVE MENT ISWI THTH EPHI LOSO PHIC ALAN DPOL ITIC
ALIM PLIC ATIO NSOF SECR ETWR ITIN GXXX

Destroy after decoding

Alan Daglish

Cryptography

What is it?
How do we do it?
Why do we need it?

First	A short history of secret writing
Second	Where we are now
Third	Where we are going

W--CO-E/ -O /TH-/ SE---T/ W-RL- /-F
INFORMATION

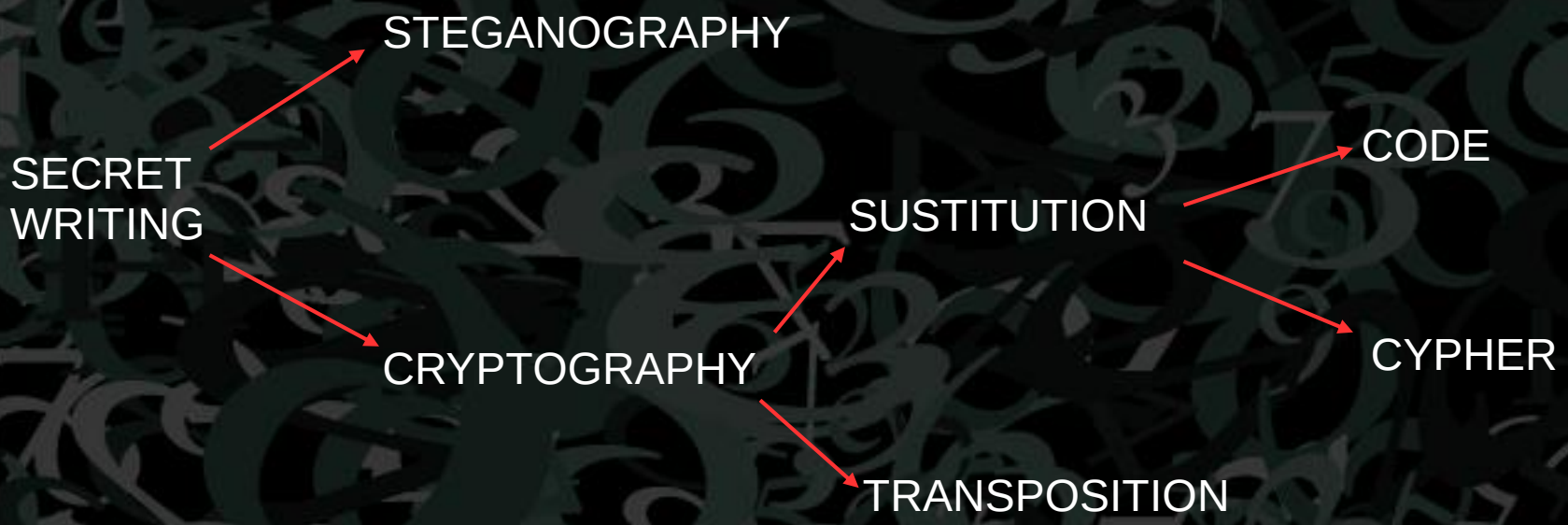
Why should I bother

Credit cards, Mobile phones, Email, Chat, Skype, Browsing, Online shopping, Cloud storage, Software updates, Online banking, Banking, Smart meters, Car keys, Electronic locks, Medical records etc etc etc.

Also Terrorists, Criminals and so on.

The Menu

This is a rough guide to the subject



Since the dawn of civilisation

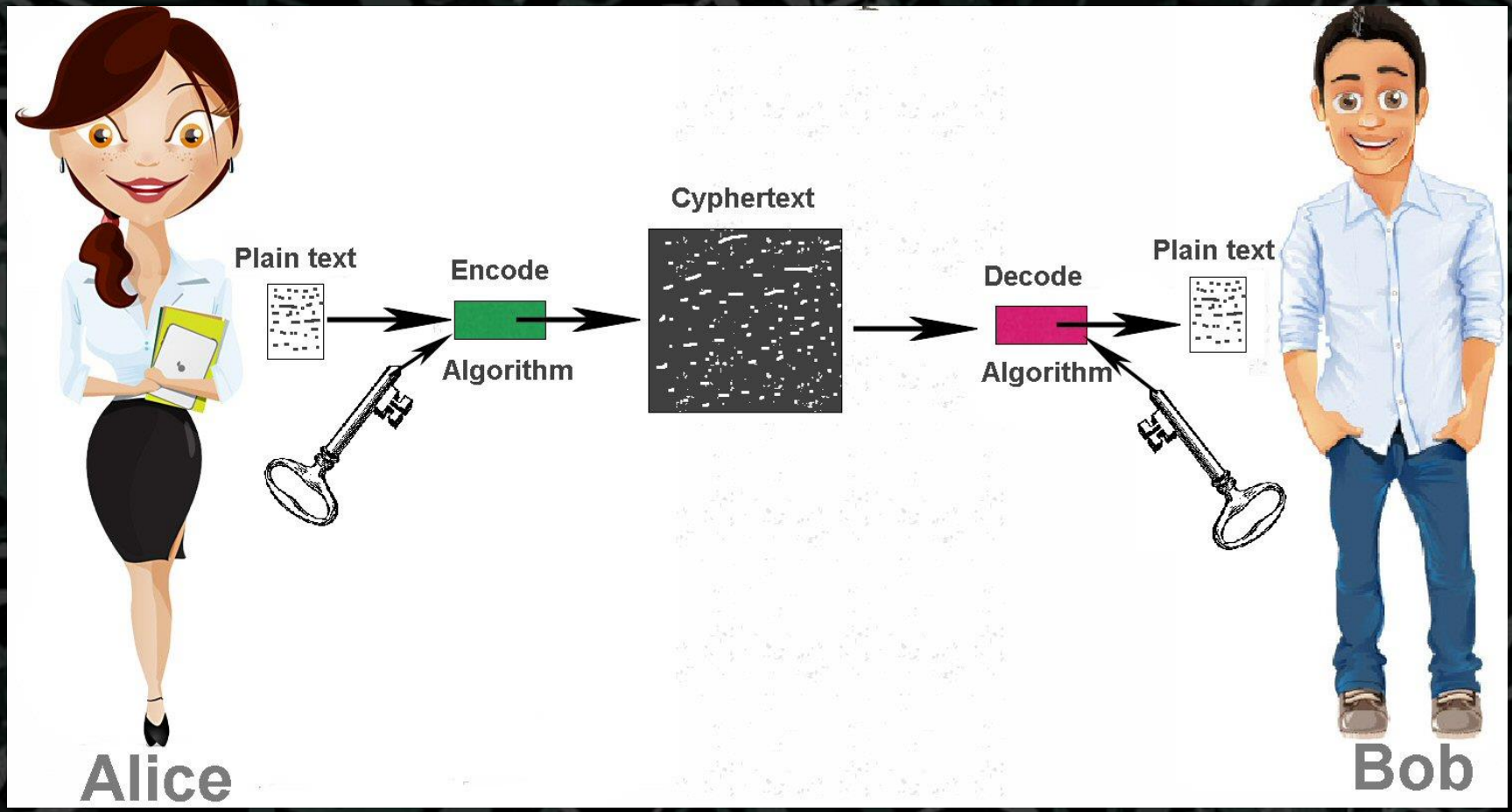
Keep it to ourselves!

The first known technique was to physically hide the message STEGANOGRAPHY

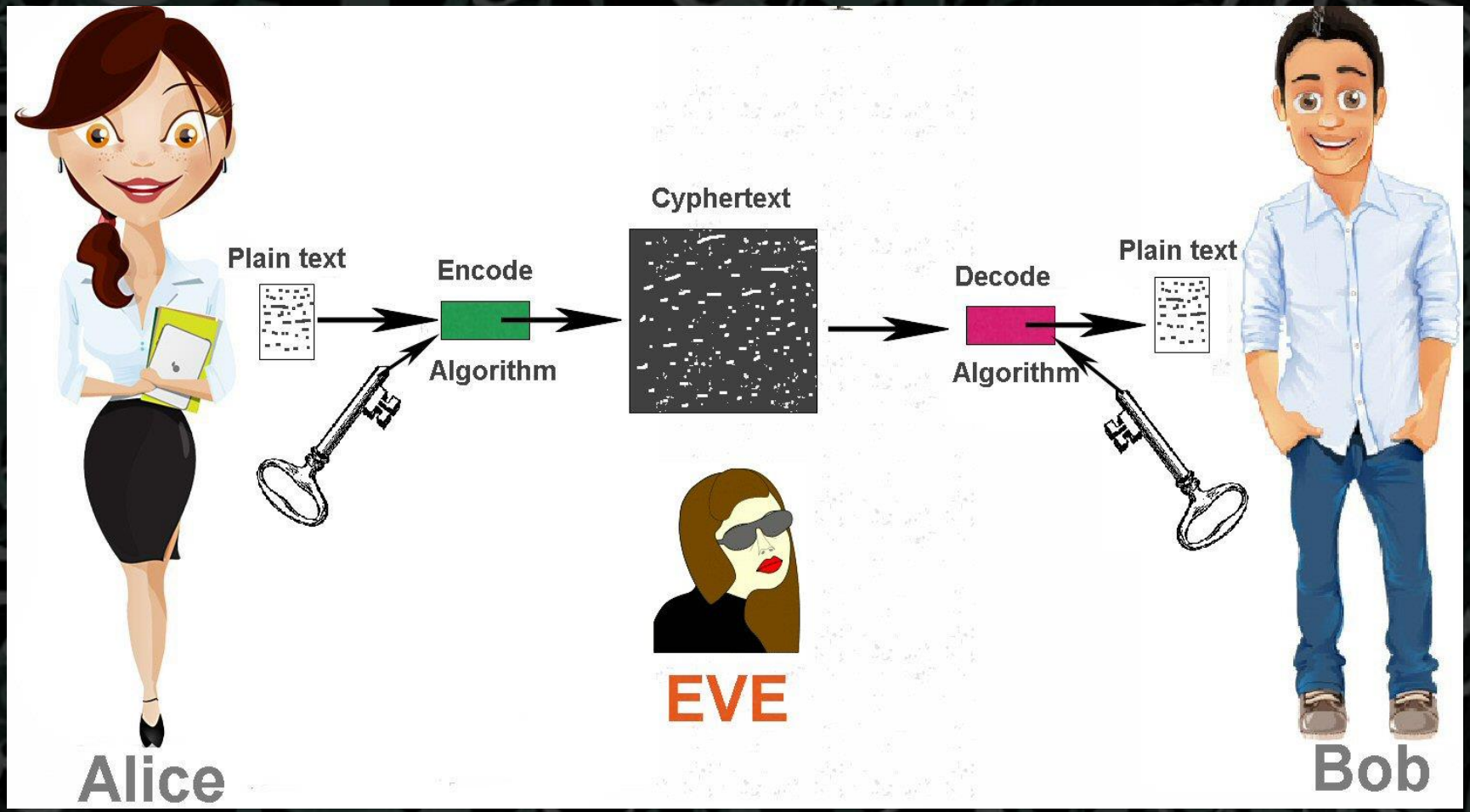
“The tattooed head” “The hollow stick” “Invisible ink” “Microdots” “Imitation objects” “Pinpricks” “body cavities” etc (more on this topic later)

However things got more sophisticated

Meet the team



And the enemy



Ancient Secrets

Babylonian Patent no 21

(Pottery Glaze Formula) C 1500 BCE

The Ancient World

The Scytale or “Spear” Transposition cyphers

Lysander of Sparta (404 BC)

The Karma Sutra Substitution cyphers

Vatsyayana (4th century AD)

Originally 4th centuryBC

The Hindus invented Book Codes

The Japanese and Chinese used syllabic codes

Now the Romans

One of the earliest cyphers we have details of is the simple substitution cypher

abcdefghijklmnopqrstuvwxyz
defghijklmnopqrstuvwxyzabc

Can you spot the pattern?

This is known as the Caesar shift (Named after Who?)

How about

abcdefghijklmnopqrstuvwxyz

cfiloruxadg.....

Just give up?

To make life harder you can just randomise the substitution alphabet and you get....

400 000 000 000 000 000 000 000 000

(4*10^26 approx) possible combinations

Question 1: At 1000 per second how long would it take to try every combination?

(answers by email please)

PS Age of universe is 4*10^17 seconds

The answer is statistics

OK so how ?

The answer was provided by the Arab scientist and philosopher AL KINDI writing in the 9th century

We know it as frequency analysis

Question 2: What are the two commonest letters in the English language?.

The answer is statistics

OK so how ?

The answer was provided by the Arab scientist and philosopher AL KINDI writing in the 9th century

We know it as frequency analysis

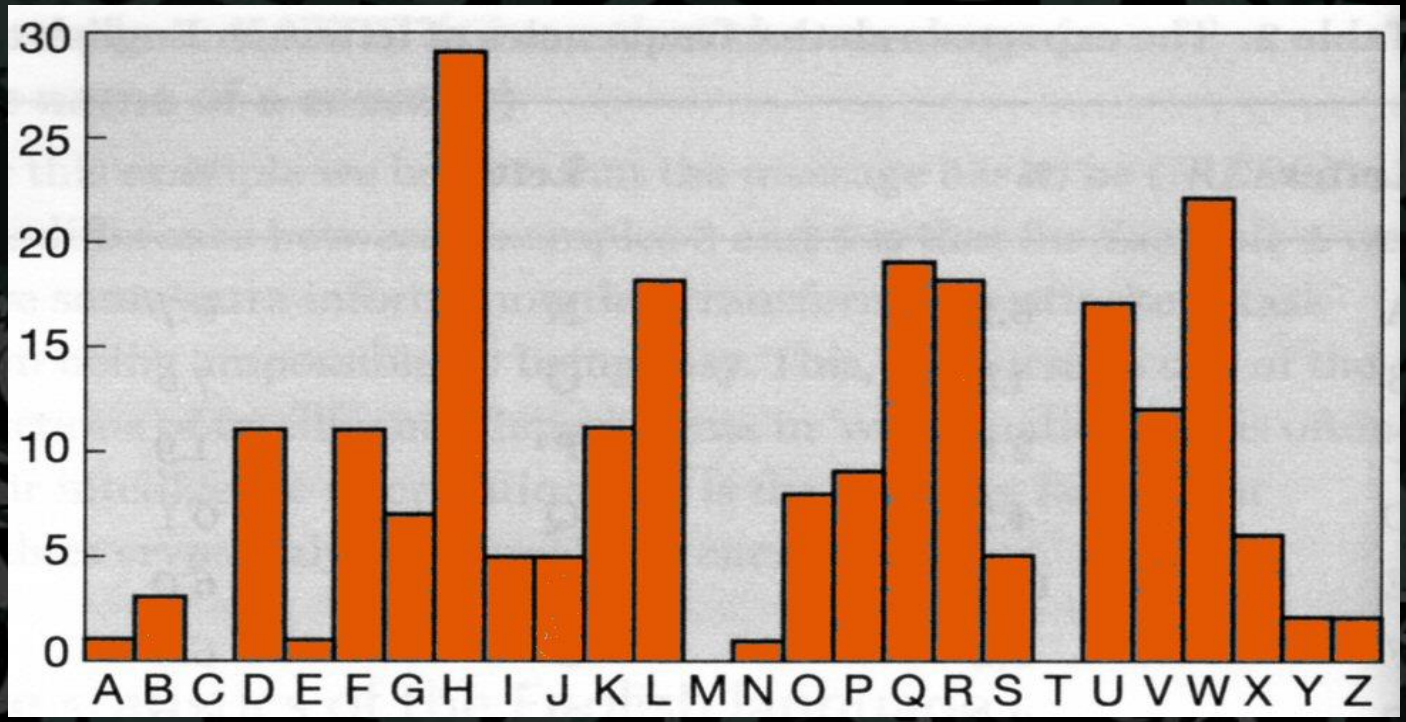
Question 2: What are the two commonest letters in the English language?.

E T A O N I S R H

Easy or what?

Below is a frequency count from a message

Can you spot the pattern?



Making life harder

OK that takes care of simple substitution cyphers so what is the next step in the 'Arms Race' NUMBERS!

An early attempt was to use bi-grams of which there are 676 using the Latin alphabet.

	A	B	C	D
A	27	114	199	13
B	33	401	55	601
C	205	177	301	10
D	514	19	97	215

Ie BDCA would be

19 199

Not yet good enough

But..... extended frequency analysis and considerable patience proved the system to be breakable.

A serious problem... it was realised that by using numbers you could create a cypher with a flat frequency distribution i.e. using multiple numbers for 'e' and 't'

However given sufficient message length and time patterns could be deduced.

Much used

As well as substitution cyphers there are TRANSPOSITION cyphers

N	O	W	I	S
T	H	E	T	I
M	E	F	O	R
A	L	L	G	O
O	D	M	E	N

This translates to:-

NTMAOOHELDWEFLMITOGESIRON

Easy to crack if you guess the grid size but combined with substitution it becomes harder (super encryption)

The next step

The next step in cyphers came in about 1500 when more complex means were devised to create cryptograms.

The Italian Vignere gave us

POLYALPHABETIC cyphers

OK try your hand on the next slide!

A Simple Vignere Cypher

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

Text is ALAN

Keyword is HELP

Cypher is

HPLC

Polyalphabets ?

Why not use scrambled alphabets?.

Ok for few users but not for lots, Eve only has to capture 1 set and they all have to be changed.

Easier is to use a standard layout and distribute keywords only

The Grand Chifre

More complex polyalphabetic cyphers were developed with elaborate scrambling rules

Prominent were the Rossignols, father and son, cryptographers to Louis XIV

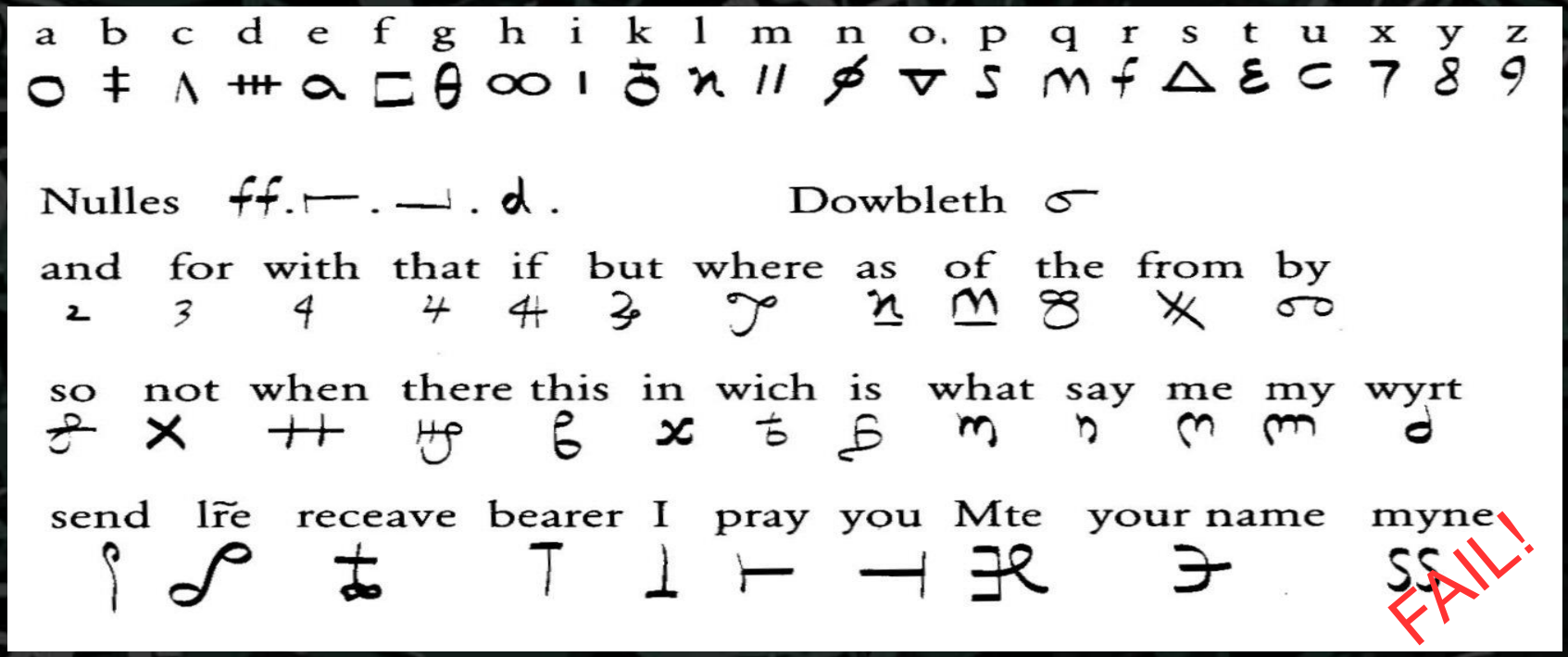
These proved unbreakable at the time

Vignere cyphers were only cracked in 1854 by Babbage and Kasiski.

Complete decipherment of the 16th cent Rossignol cypher was only achieved by Baziers in 1892

All Greek to me

Mary Queen of Scots tried everything



Sherlock Holmes The Adventure of the Dancing Men

Codes

As expertise in decryption increased the use of codes became more and more necessary.

Codes substitute groups of letters or numbers for words or phrases.

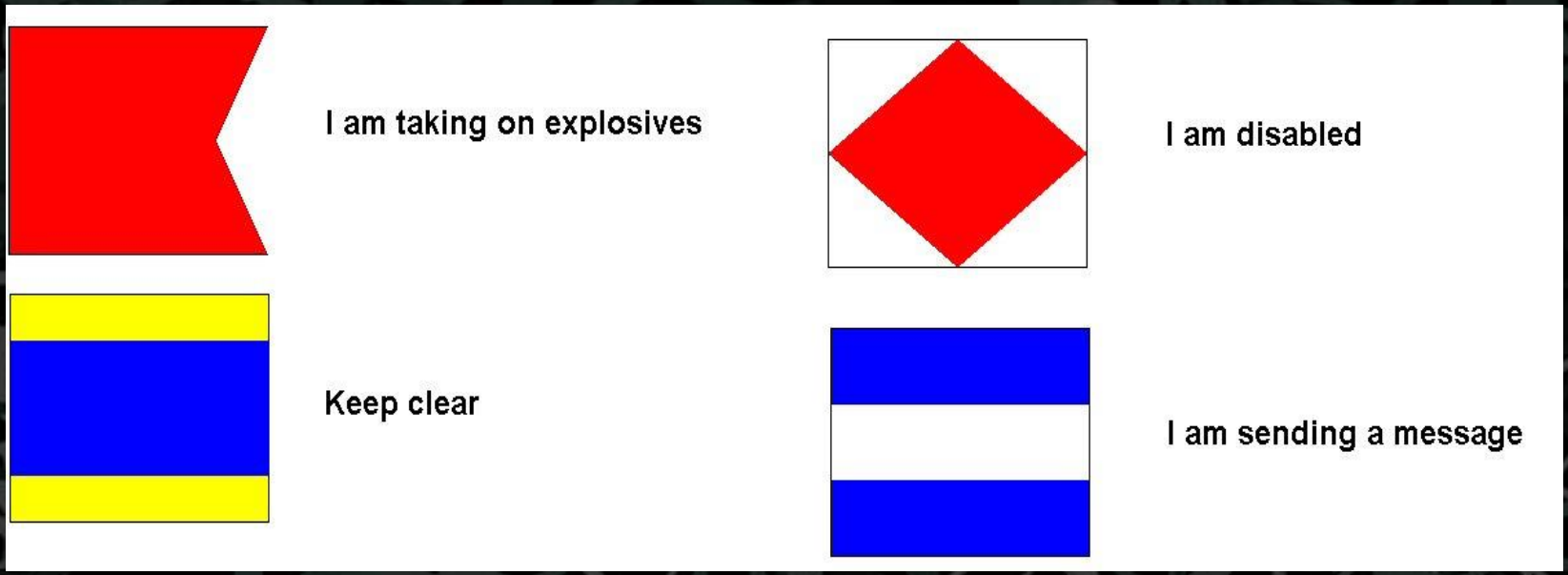
The advent of the telegraph led to the creation of public commercial telegraphic codes(ABC, Bentley)

i.e. ZXPRC = “Attack at dawn”

EBNET = “The Captain is insane”

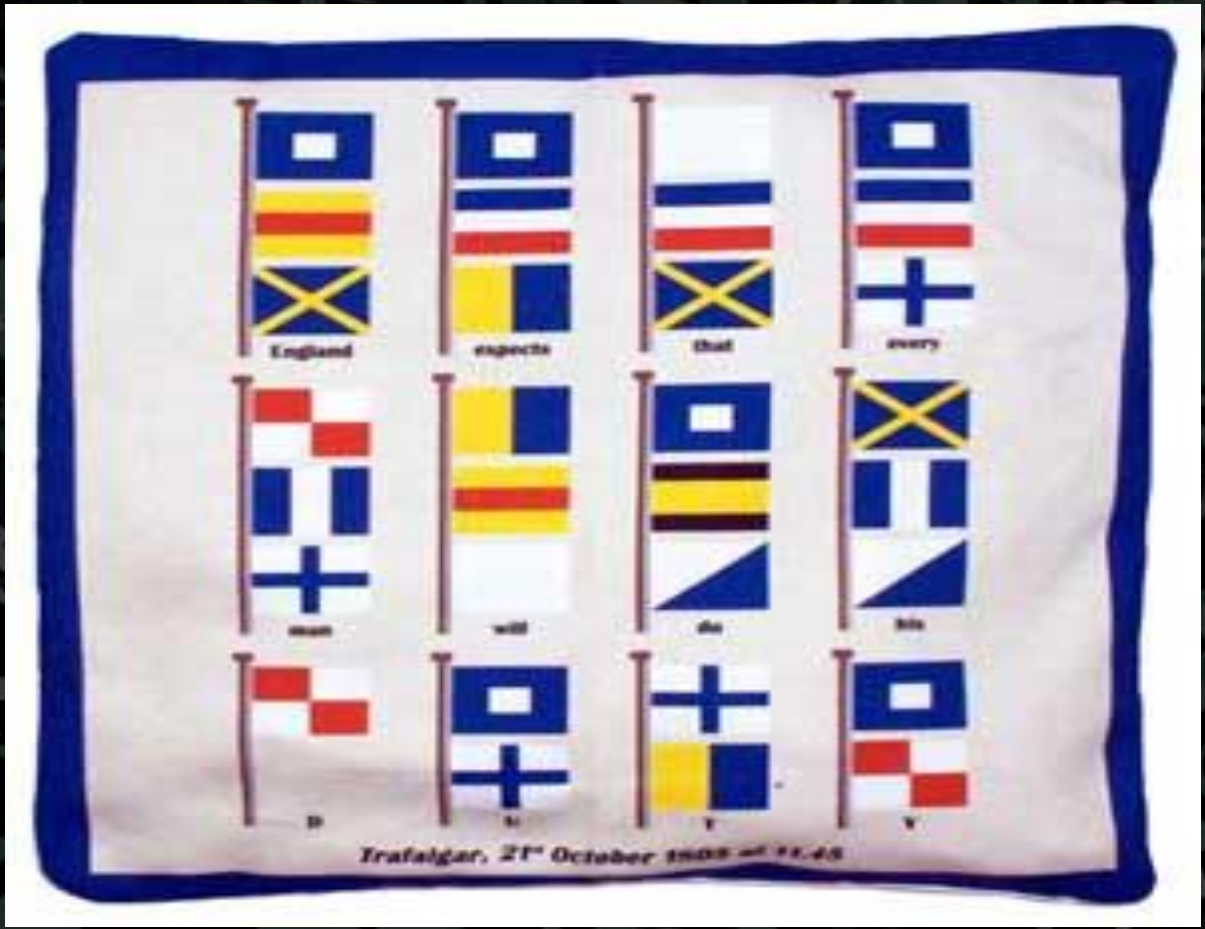
Common Codes

Many varieties of code were devised. We are used to this in things like naval flag codes



And of course

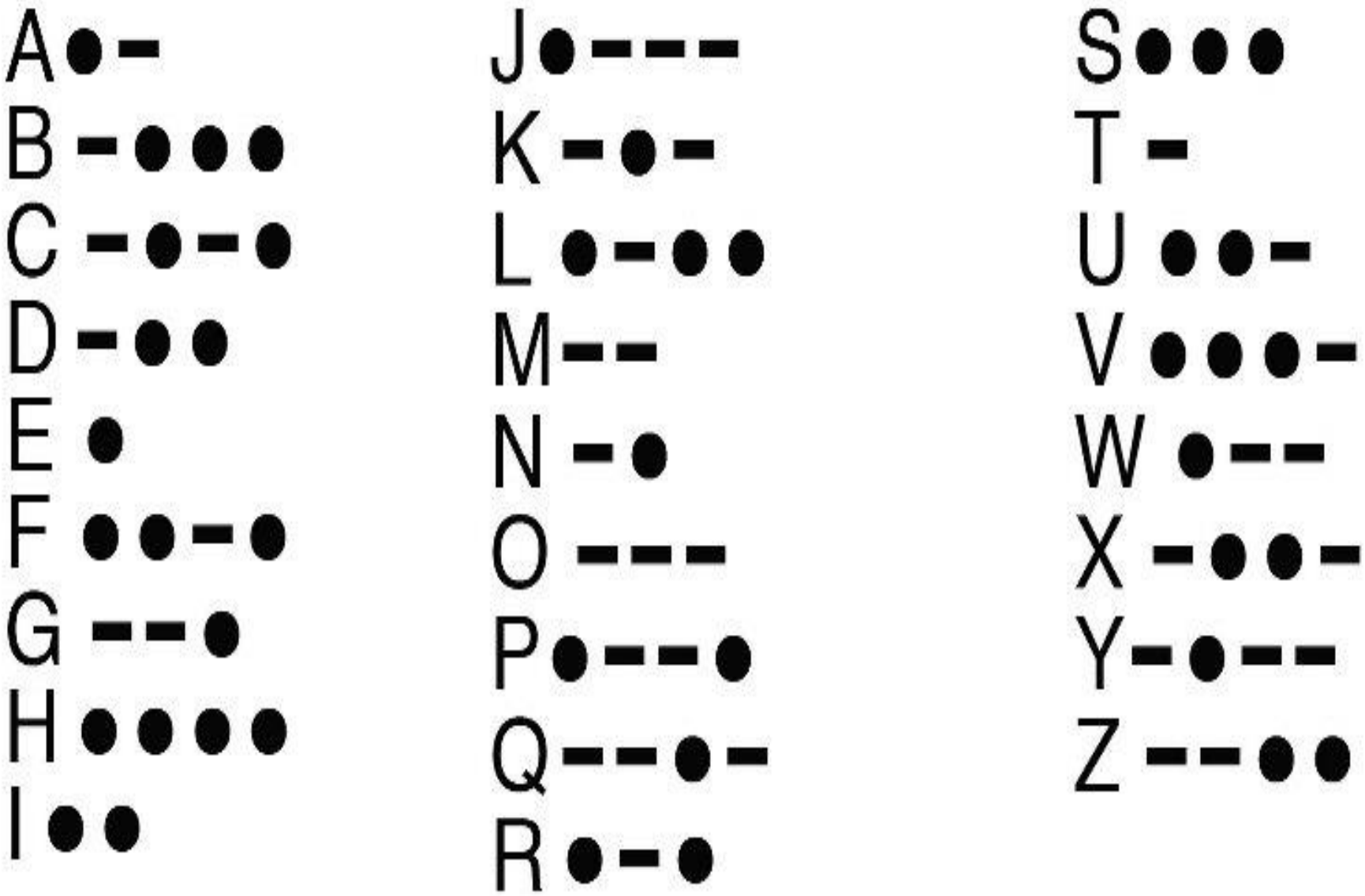
England expects every man.....



Mor e Code

Probably the the code most familiar to us all

10 01 110 111 000 001 101


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

Unfinished Business

There are some things not yet deciphered.

- The Voynich manuscript
- The Beal papers
- D-Day Carrier pigeon
- Zodiac Killer

Time is critical

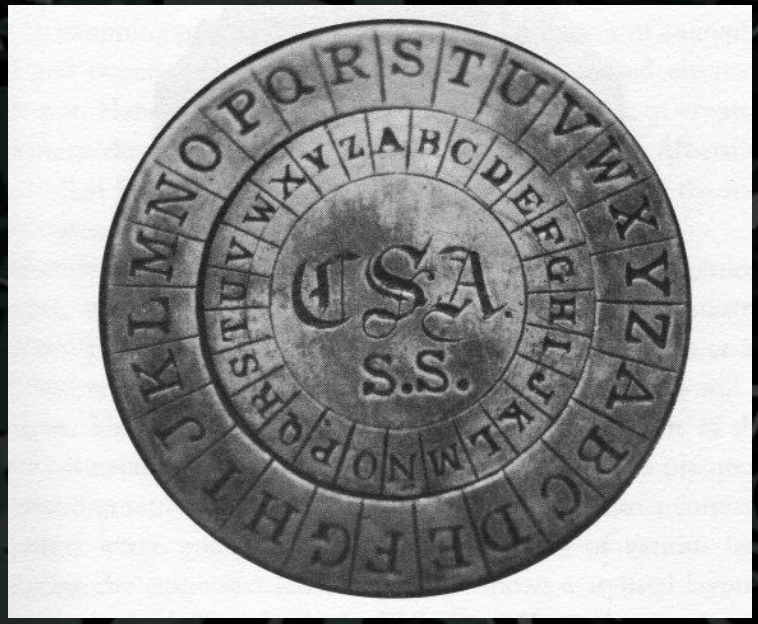
As cyphers became more complicated they became harder to crack but the time for Alice to encrypt and Bob to decrypt became longer and longer.

This could be a problem in the military situation when information is time critical.

The answer is mechanisation.

Southern Knowhow

Cypher discs were used by the South in the US civil war and could be used to generate polyalphabetic messages by rotating the disc after each letter according to a set pattern.



A Breakthrough

During the first world war cryptography assumed increased importance due to the use of radio which meant messages were easier intercepted.

The cyphers in use were variations on the traditional but in 1928 a purely mathematical cypher was devised based on matrix algebra. The system was cracked two years later but it had opened a window.

Mechanisation

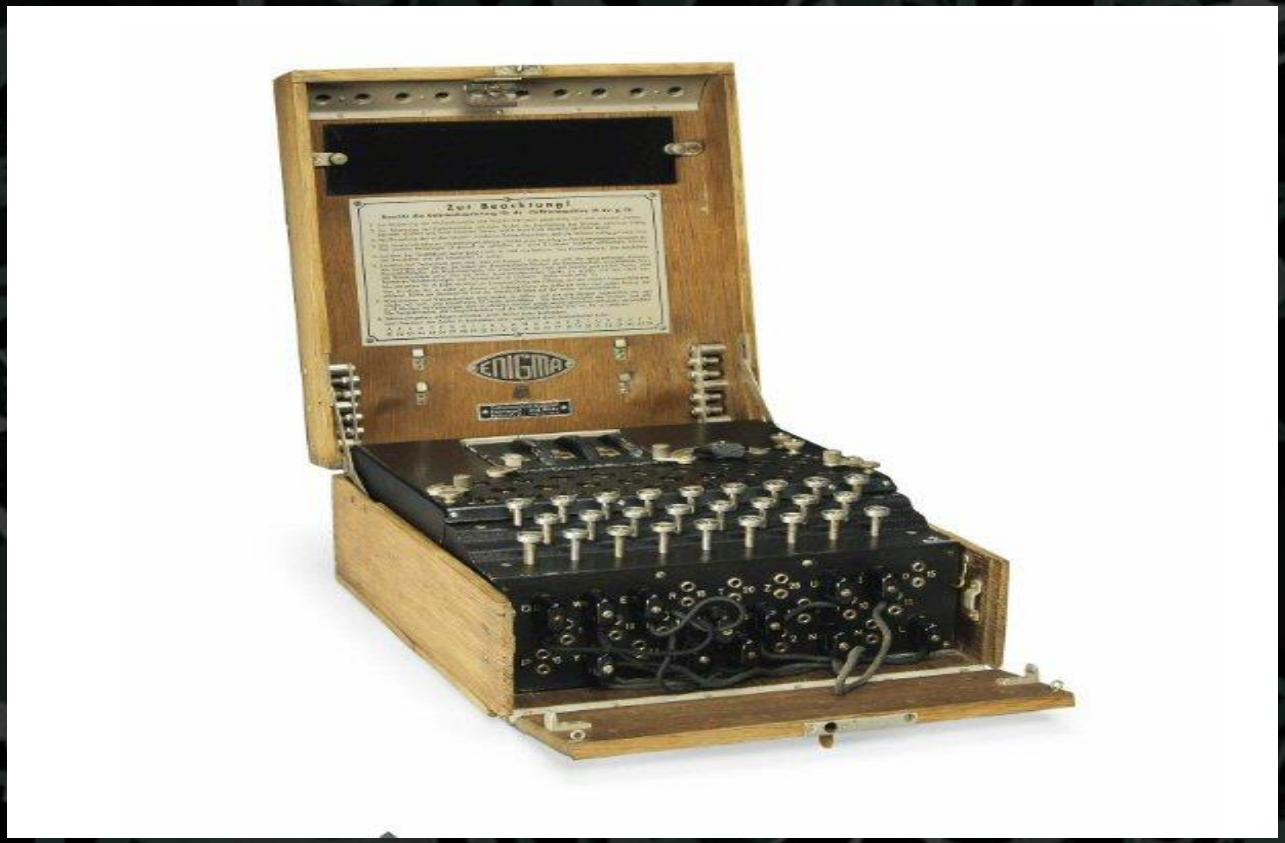
Mechanisation took a great stride forward with the patenting in 1918 by Arthur Scherbius of the first really successful mechanised system, based on a typewriter keyboard and a huge keyspace

This was the by now famous ENIGMA machine.

It did however take until 1936 to make an impact when adopted by the military

WWII

The ENIGMA Cypher machine



The impossible task

This was regarded as the ultimate polyalphabetic cypher.

Total number of keys was in excess of

10 000 000 000 000 000 combinations

Considered absolutely unbreakable by the German military in WWII

FAIL

British is best

The Typex machine, in use up to 1950's

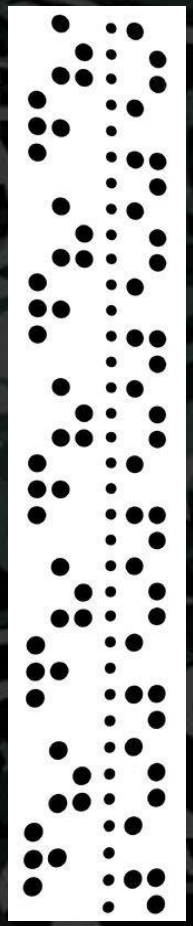
A Step Further

Even though they regarded the Enigma as unbreakable the German High command demanded a means of secure communication which was less time consuming and needed fewer eyes on the message

The answer was a modified Teletype machine known as the Lorenz SZ40.

Explanation follows.....

A Mathematical Machine



Basically the modified machine used a 5 bit code and produced a tape that was fed back into the machine and sent by some means or other.

The Lorenz modified the code by adding a number to each character in a method known as “no carry adddition” or as we know it “exclusive or”

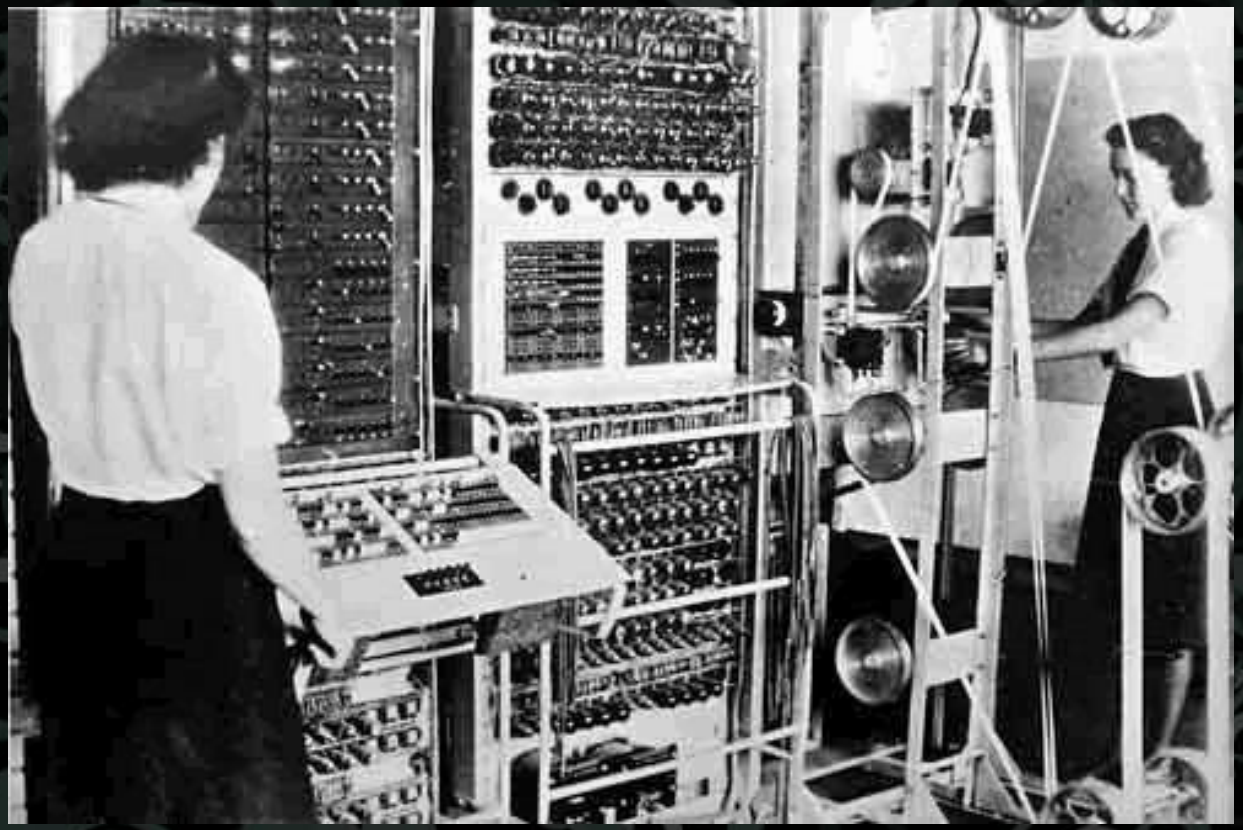
Under the Hood

Technical stuff (using ASCII 7 bit codes)

- Plaintext HELP = 72 69 76 80 ascii character codes
- = 1001000 1000101 1001100 1010000 1 is a hole, 2 is a blank
- Keyword text SAVE = 83 65 86 69 (usually 40 characters)
- = 1010011 1000001 1010110 1000101
- Rule if bits the same result is 0, if different the result is 1
- Do it, going from left to right
- = 0011011 0000101 0011010 0010101
- Result is gibberish if converted back to letters
- BUT simply applying the same rule to it using the keyword restores the original text.....check for yourself with any number

The Second Dawn

It took the invention of what is demonstrably the first programmable computer to break the Lorenz cypher. It also took a lot of luck.



The Cold War Era

After the war cryptographers continued to use both computerised Enigma based methods and Lorenz style encoding. (AES was a standard)

Digital encoding depended for its secrecy on having long random keys.

Much cryptographic research went into random number generation.

Still absolute secrecy depended on the “One time pad” (and still does)

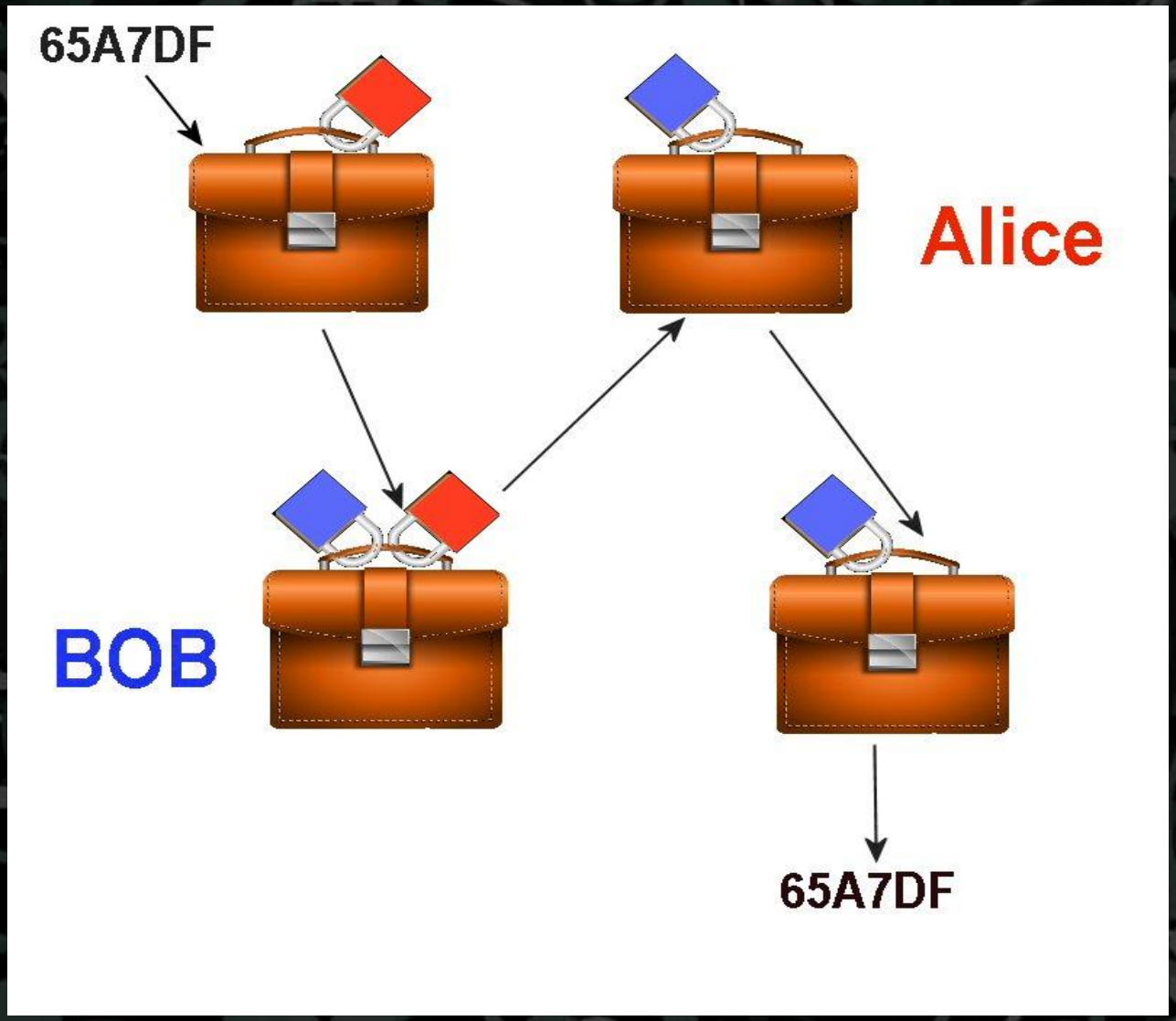
The key problem

There is a problem.

Your messages could be made reasonably secure providing you could prevent Eve from getting hold of the encryption key.

A large organisation might have to frequently distribute thousands of keys by the only(expensive) secure method, i.e. courier

Diffie-Hellerman



The Big Step Forward

Public key encryption

The best known was invented by Rivest, Shamir and Aldeman in 1978 (RSA) (Actually by a Brit, James Ellis, at GCHQ, but that is another story)

Relies on a 'trapdoor' function, that is a function which uses an encryption key that is totally different from the decryption key(Asymetric).

RSA Cryptography

The security of the system relies heavily on the difficulty of factoring very large numbers.

The public key is generated by multiplying two very large (secret) primes together.

Encryption is done using the key and modular arithmetic. Decryption relies on knowing what the primes were.

To find the large primes used even on today's computers is an “Age of the universe” problem.

The Basics

Just a quick note on Modular Arithmetic

- If we divide 22 by 7 we get 3.143.....
- If we did this in school before we learned decimals we got 3 remainder 1
- Similarly 31/5 is 6 remainder 1
- Usually 77 |6| = 5 or 77 mod6 = 5

If all we know is the remainder there is no way to recover the two numbers involved

A worksheet on RSA is available afterwards

Not the final answer

The problem with RSA is the time it takes to encrypt and decrypt as complicated algorithms are needed to handle the very large numbers.

Many systems use a combination of public key and symmetric keyword cyphers, the public key being used to send the encrypted keystring.

The current AES standard is based on matrix algebra and was developed by Rijndael(2002)

Elliptic curve cryptography

This is a highly mathematical way of generating encryption keys based on elliptic curves

It has the advantage of using smaller keys than RSA for the same security and, as it works on smaller numbers, is considerably faster

It is widely used in mobile communications.

A Cheap Timeless Alternative

At the end of WWI the One Time Pad' was devised.

One time pads were literally notepads with a string of random characters on them. These were in fact very long keystrings. These were used in conjunction with a Vignere grid.

Pads are used once and discarded.

Using the pads once ensured no depth!

Making a Hash

Hashing is a way of turning text into a unique number. It forms the basis of several cryptographic standards

Extensively used for passwords and digital signatures

i.e. to hash “the” = t*13+h*127-e*3 = 14413

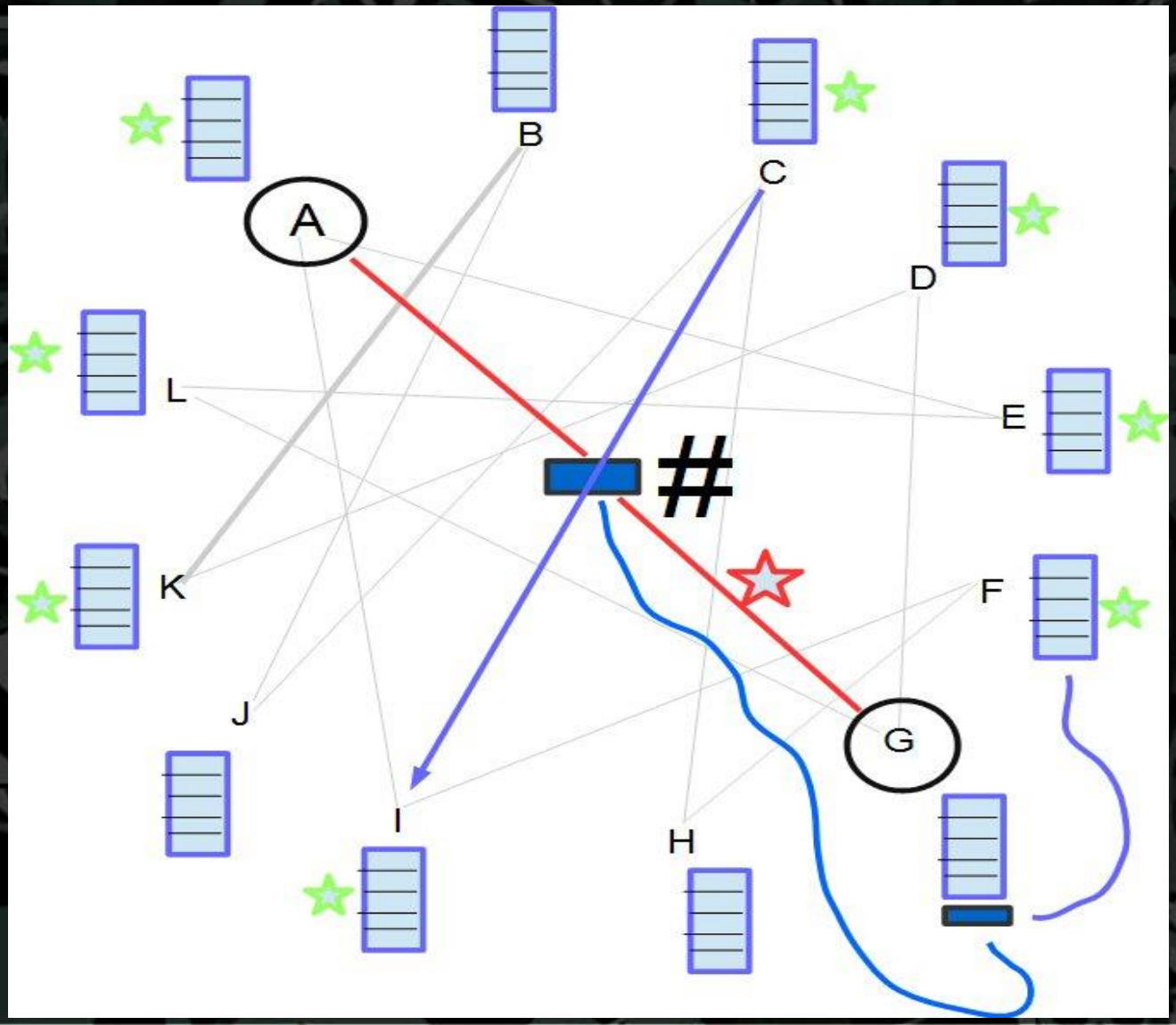
The SHA-3 standard uses a combination of 'And', 'Xor', 'Rot' and 'Not' and is very difficult to break

Two examples Liverpool Scibar and Liverpool scibar

E42D915B4B11E54E625904D719F874CD4CCC91AB

1206F1F190D71DE92B3CB366B3695683948E1B85

Crypto Coinage



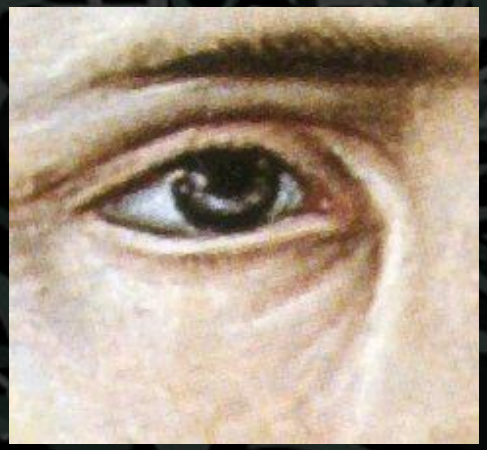
Passwords

Passwords you send over the net are hashed before sending and the hashes are stored with your personal information.

Lists of 2+ million passwords are available for sale on the dark net. They can be easily hashed and compared rather than decoded

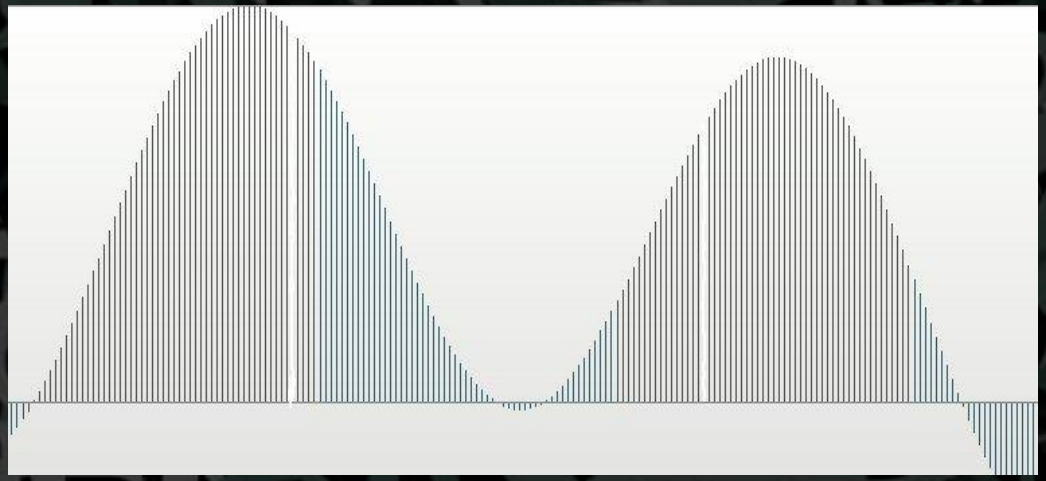
The answer is random characters, the problem is memory!

Steganography revisited



A 24 bit .BMP image

The rhs has all the LSB equal to 1



A 400 hz sine wave with samples missing

(440 khz sampling)

Steganography hidden all around us

- Watermarking
- Terrorist activity(9/11)
- Copyright protection
- HP and Xerox Laser Printers

Where we are

Are we all done then?

The answer at the moment is yes.....but....

All systems depend for their security on the correct implementation(And honest cryptographers).

It should be remembered that there is always a human being in the loop!

Cryptanalysts have not yet given up

Quantum Communications

Quantum Physics

It can provide secure key exchange but in limited circumstances.

Quantum computers, when they arrive will enable the very fast breaking of security keys.

When? Soon or maybe a bit longer

Quantum Communications

Quantum Physics

It can provide secure key exchange but in limited circumstances.

Quantum computers, when they arrive will enable the very fast breaking of security keys.

When? Soon or maybe a bit longer

Quantum Security

Quantum key exchange Relies on the fact that when you detect a photon you actually change a property.

Eve can intercept the key string but Bob will know this because she has randomly changed the property.

Alice tells Bob, for instance, how many 1s in the key and if Bob finds a different number he panics and tries again.

How it's done

A popular method relies on the analysis of the polarisation of photons.

Bob is made aware of the polarisation scheme but Eve has been intercepting these photons, hence altering them and cannot relate these to the key.

This method is becoming more widely used as fibre networks expand.

The future

Quantum key exchange is limited by the need for direct fibre communication, at the moment.

The Chinese have transmitted a message from Beijing to Vienna via satellite using entangled photons.

So will our communications be safe in the future.....guess

Appendix 1

Passwords and pin numbers

It is possible to buy 2 million passwords on the dark net.

Even though these are hash coded it only takes a short time to compare the password list to the hash codes you have hacked.

- USE A RANDOM LETTER PASSWORD

or else!

A good method for generating these is available afterwards

Pin Numbers

My YB pin code is 1248, for LLoyd it is 5277

My code word for YB is “help” and for lloyds is “send”. This is my encryption scheme

A 3	B 6	C 1	D 7	E 2
F 8	G 5	H 1	I 9	J 2
K 7	L 4	M 3	N 7	O 8
P 8	Q 1	R 7	S 5	T 3
U 4	V 3	W 9	X 6	Y 5

??????????????????

Sfgn wdof rtms sdft mmxz

??????????????????

Sfgn wdof rtms sdft mmxz

(Thanks for listening)

All questions in plain text please

mail@adaglish.org.uk