Secrets and Spies

Dan Goldsmith James Shuttleworth

Introduction

About Us

- Dr. Daniel Goldsmith
  - Senior Lecturer: Ethical Hacking and Cyber Security
- Dr. James Shuttleworth
  - Principle Lecturer, Lead of Coventry IoC

Ethical Hacking

- Study of Cyber Security
- Lots of interesting technical challenges to solve
- Look for flaws in systems and propose fixes
- Adversarial Mindset

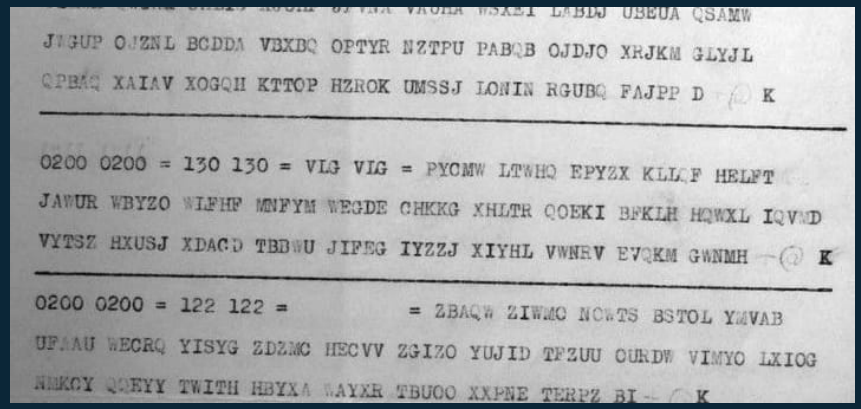
The IoC

- UK Wide initiative to increase Technology skills
- 33 UK universities involved
- Coventry University Leads focus on Industry
- https://instituteofcoding.org/

Cryptography

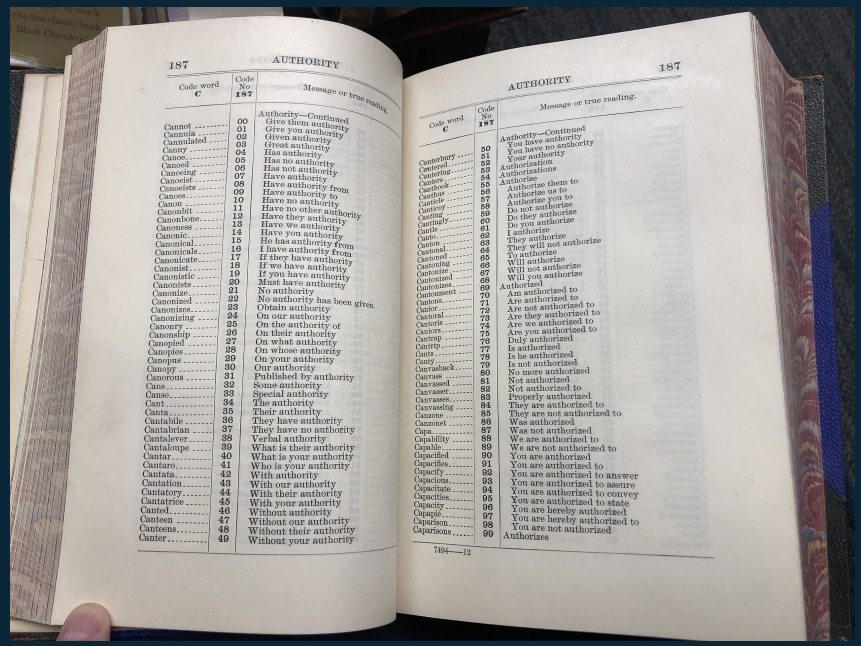
Cryptography

- Protecting Information and Data through the use of Codes and Ciphers
- If a message is intercepted, getting the meaning is difficult



Codes and Ciphers

- **Codes:** Provide a mapping between words or phrases and other symbols
- **Cipher** Used to transform one symbol into another



187 AUTHORITY

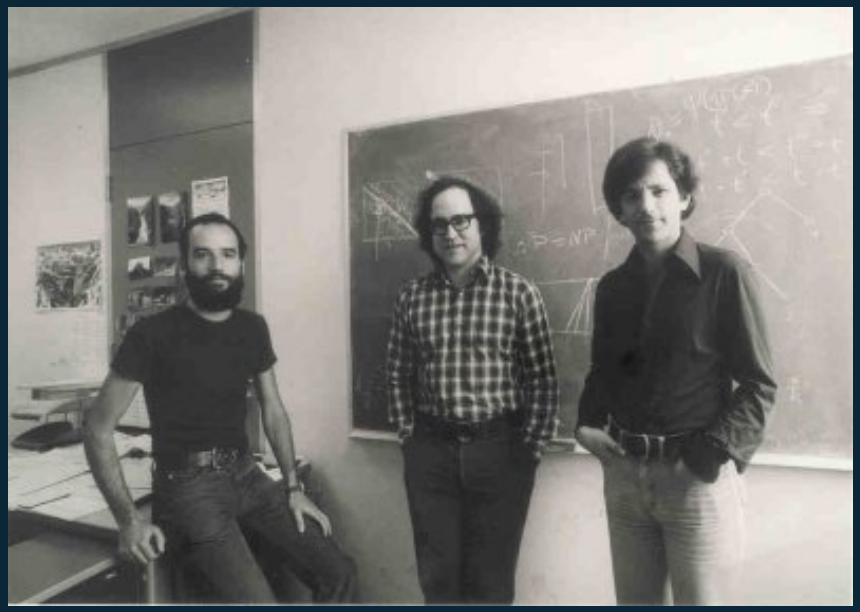
Code word. C	Code No. 187	Message or true reading.
		Authority—Continued
Cannot	00	Give them authority
Cannula	01	Give you authority
Cannulated	02	Given authority
Canny	03	Great authority
Canoe	04	Has authority
Canoed	05	Has no authority
Canoeing	06	Has not authority
Canoeist	07	Have authority
Canoeists	08	Have authority from
Canoes	09	Have authority to
Canon	10	Have no authority
Canonbit	11	Have no other authority
Canonbone	12	Have they authority
Canoness	13	Have we authority
Canonic	14	Have you authority
Canonical	15	He has authority from
Canonicals	16	I have authority from
Canonicate	17	If they have authority
Canonist	18	If we have authority
Canonistic	19	If you have authority
Canonists	20	Must have authority
Canonize	21	No authority
Canonized	22	No authority has been given
Canonizes	23	Obtain authority
Canonizing	24	On our authority
Canonry	25	On the authority of
Canonship	26	On their authority
Canopied	27	On what authority
Canopies	28	On whose authority
Canopus	29	On your authority
Canopy	30	Our authority
Canorous	31	Published by authority
Cans	32	Some authority
Canso	33	Special authority
Cant	34	The authority
Canta	35	Their authority
Cantabile	36	They have authority
Cantabrian	37	They have no authority
Cantalever	38	Verbal authority
Cantalope	39	What is their authority
Cantar	40	What is your authority
Cantaro	41	Who is your authority
Cantata	42	With authority
Cantation	43	With our authority
Cantatory	44	With their authority
Cantatrice	45	With your authority
Canted	46	Without authority
Canteen	47	Without our authority
Canteens	48	Without their authority
Cantet	49	Without your authority

AUTHORITY 187

Code word. C	Code No. 187	Message or true reading.
		Authority—Continued
Canterbury	50	You have authority
Canterel	51	You have no authority
Cantering	52	Your authority
Canthook	53	Authorisation
Canthus	54	Authorizations
Cantico	55	Authorize
Cantile	56	Authorize them to
Cantivy	57	Authorize us to
Cantlet	58	Authorize you to
Cantlings	59	Do not authorize
Cantline	60	Do they authorize
Cantle	61	Do you authorize
Canto	62	I authorize
Canton	63	They authorize
Cantonal	64	They will not authorize
Cantoned	65	To authorize
Cantoning	66	Will authorize
Cantonize	67	Will not authorize
Cantonized	68	Will you authorize
Cantonizes	69	Authorized
Cantonment	70	Am authorized to
Cantons	71	Are authorized to
Cantor	72	Are not authorized to
Cantoral	73	Are they authorized to
Cantoris	74	Are we authorized to
Cantors	75	Are you authorized to
Cantrap	76	Duly authorized
Cantrip	77	Is authorized
Cants	78	Is he authorized
Cantz	79	Is not authorized
Canvasback	80	No more authorized
Canvass	81	Not authorized
Canvassed	82	Not authorized to
Canvasser	83	Properly authorized
Canvasses	84	They are authorized to
Canvassing	85	They are not authorized to
Canzone	86	Was authorized
Canzonet	87	Was not authorized
Cnpa	88	We are authorized to
Capability	89	We are not authorized to
Capable	90	What is authorized to
Capacified	91	You are authorized
Capacifies	92	You are authorized to
Capacify	93	You are authorized to answer
Capacious	94	You are authorized to assure
Capacitate	95	You are authorized to convey
Capacities	96	You are authorized to state
Capacity	97	You are hereby authorized
Capagis	98	You are hereby authorized to
Caparison	99	You are not authorized
Caparisons		Authorizes

7494—13

Cryptographers VS Cryptanalyst



Cryptographers: RSA

Cryptanalyst: Dilly Knox

Early Crypto

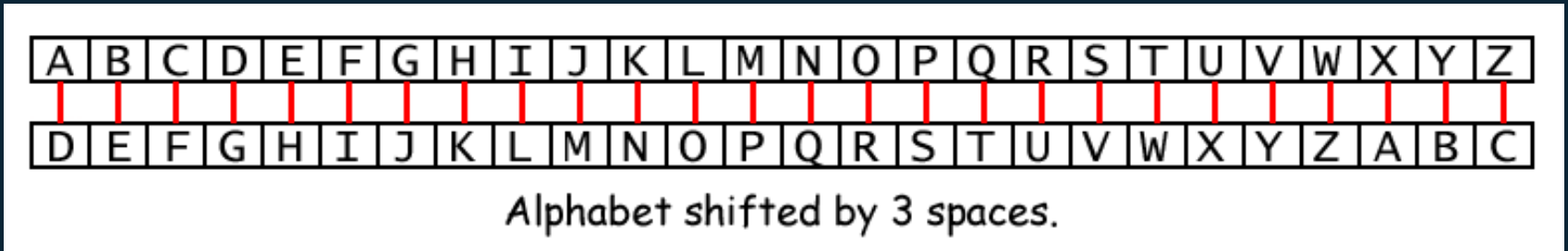
The Ancient World

- Shaving the Head of Slaves
- Scytale
- Atbash

How many bowls of cereal did Caesar have for breakfast?

Cipherdisc

Caesar Cipher

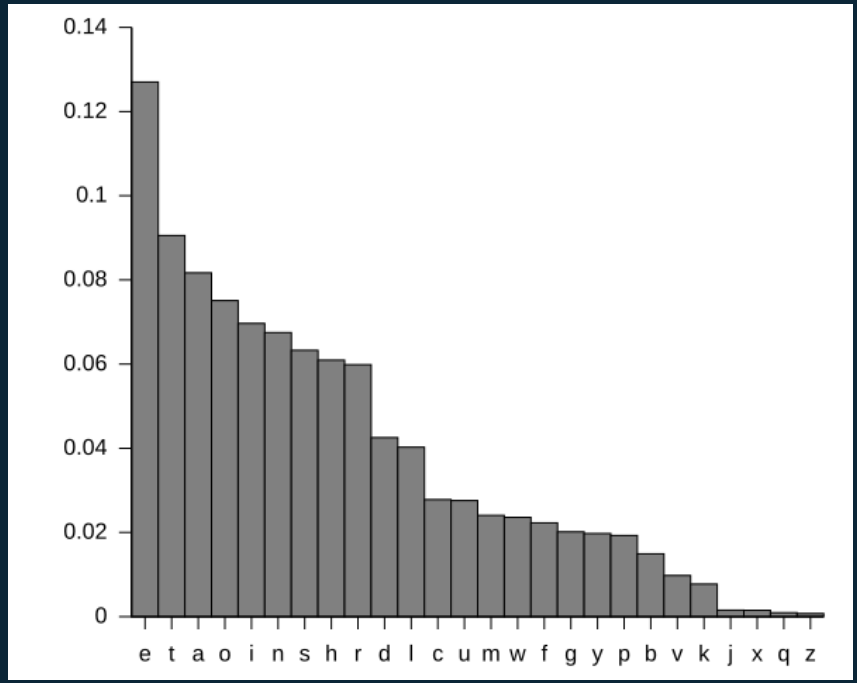


Caesar Shift

Plaintext	Veni Vidi Vici
Ciphertext	YHQL YLGL YLFL

Al-Kindi and the first Cryptanalysts

- First description of Frequency analysis published around 800AD
- Look at frequency of Letters in ciphertext
- Use these for Clues to the plaintext



Simple Cryptanalysis Demo

```
GUR FXL NOBIR GUR CBEG JNF GUR PBYBE BS GRYRIVFVBA
GHARQ GB N QRNQ PUNAARY
```

- What patterns can we see:
  - R and G Most common Letters (E and T)
  - 3 * GUR
  - 1 * N
  - BS and BG

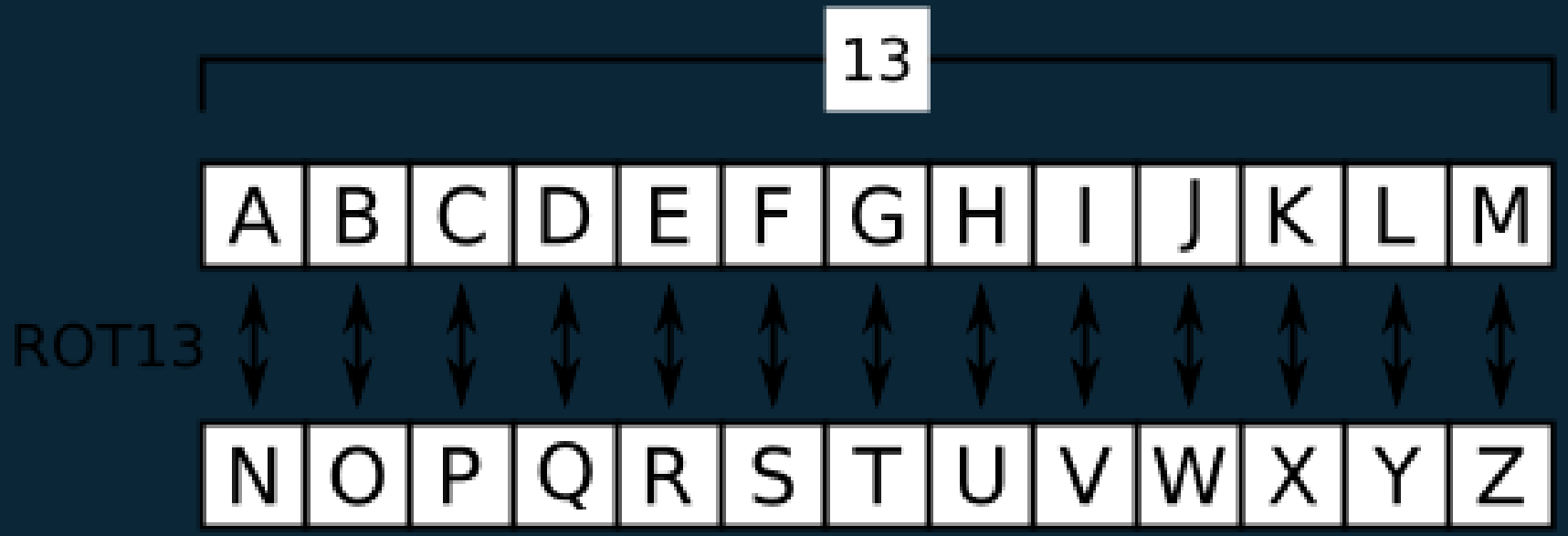
Simple Cryptanalysis

- Most common 3 letter words
  - the, and, for, are, but

`THE fxl nobiE THE cbeT jnf THE pbybe bs TEyEivfvba`

`ThaEq Tb n qEnq pHnaaEy`

Simple Cryptanalysis



Rot13

```
the sky above the port was the color of television
tuned to a dead channel
```

‘the indecipherable cipher’

- “Viginere” Cipher
- Multiple alphabets used for substitution
- Frequency Analysis much harder, as the basis shifts

	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	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

Viginere Example

- We first select a key used to encipher the message. For example “TURING”
- Use the Letter in the Key, to select the alphabet to use

Message	SUPER SECRET MESSAGE
Key	TURIN GTURIN GTURING

Viginere Example

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

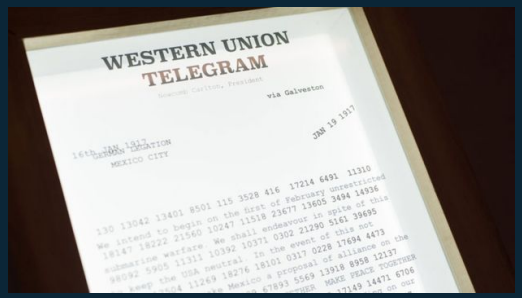
Message	SUPER SECRET MESSAGE
Key	TURIN GTURIN GTURING
Ciphertext	LOGME YXWIMG SXMJITK

Analysis of Viginere

- Relies on the cyclic nature of the Key
- Look for repeated groupings of letters in the ciphertext to guess key length
- Frequency analysis on the groups of letters to guess likely keys

The 20th Century and World Wars

Communications become more important (and easier to intercept)

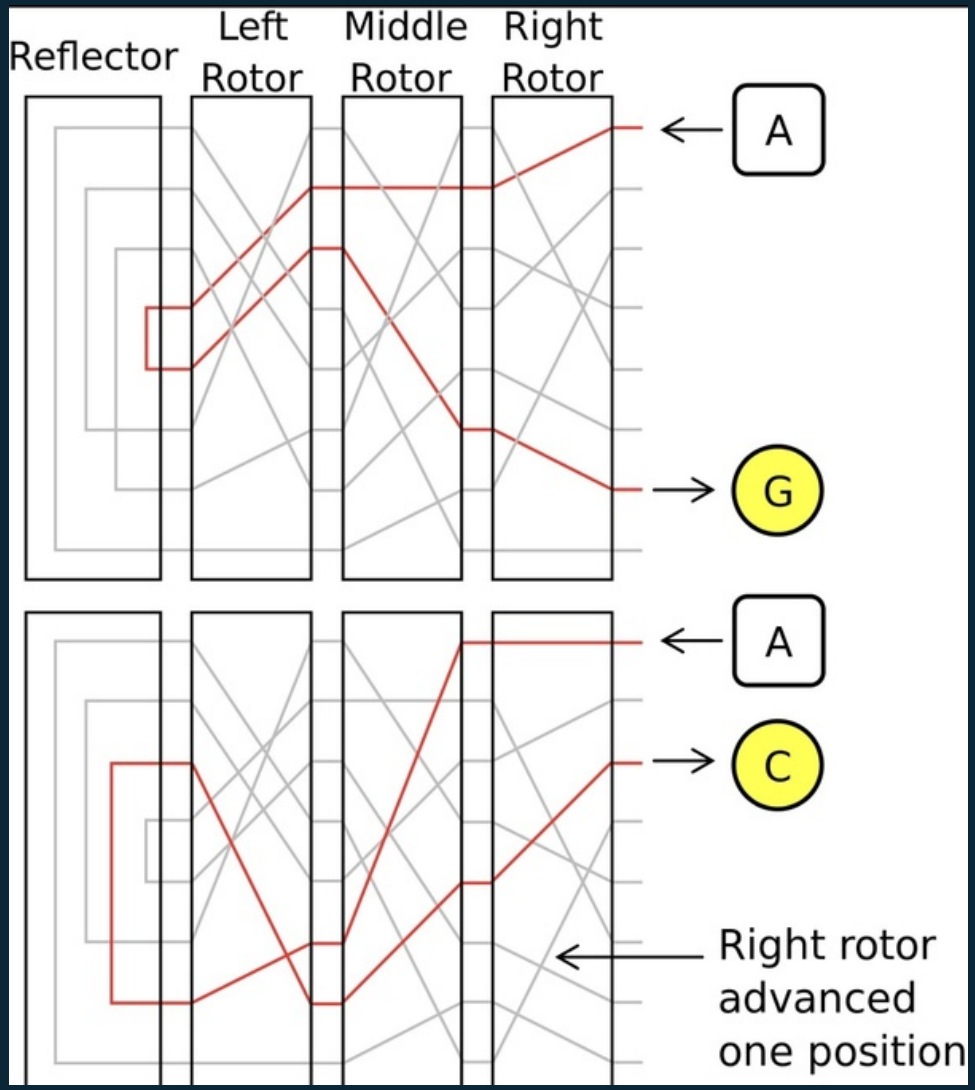


- Invention of modern electronic communication, increased the need for security:
  - Telegraph
  - Radio
- Cryptography also became Mechanised

Enigma

Enigma Machine

Enigma



Enigma Encoding

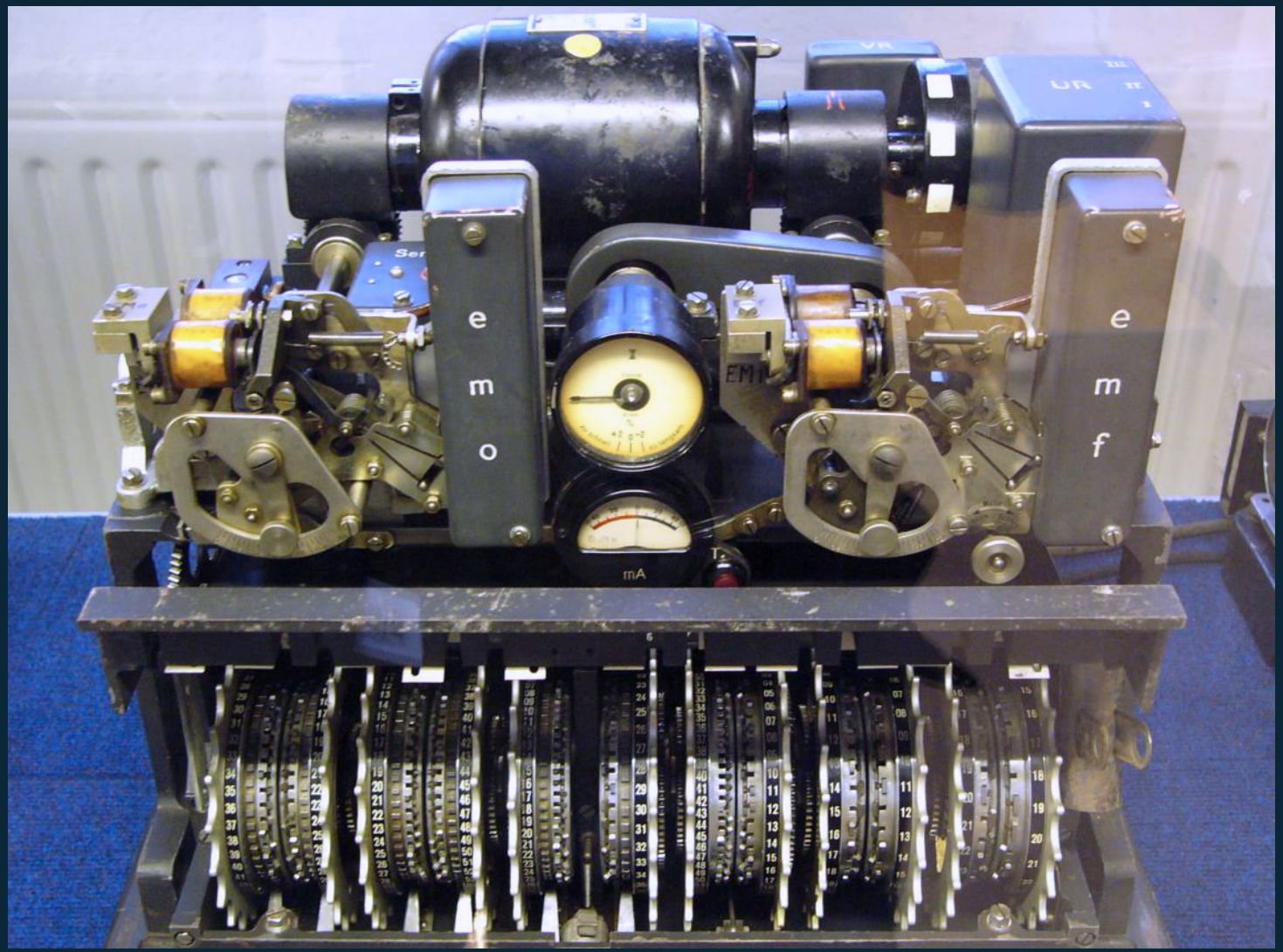
Breaking Enigma

- How to break 158,962,555,217,826,360,000 possible settings?
- Luck, Poor operating practice, Espionage, and a tonne of hard work.
  - Rejewski and the Polish Cipher Bureau
  - Alan Turing and Bletchly park
- Cribs to guess part of the plain text and get a handle on the encoding.

The Bombe

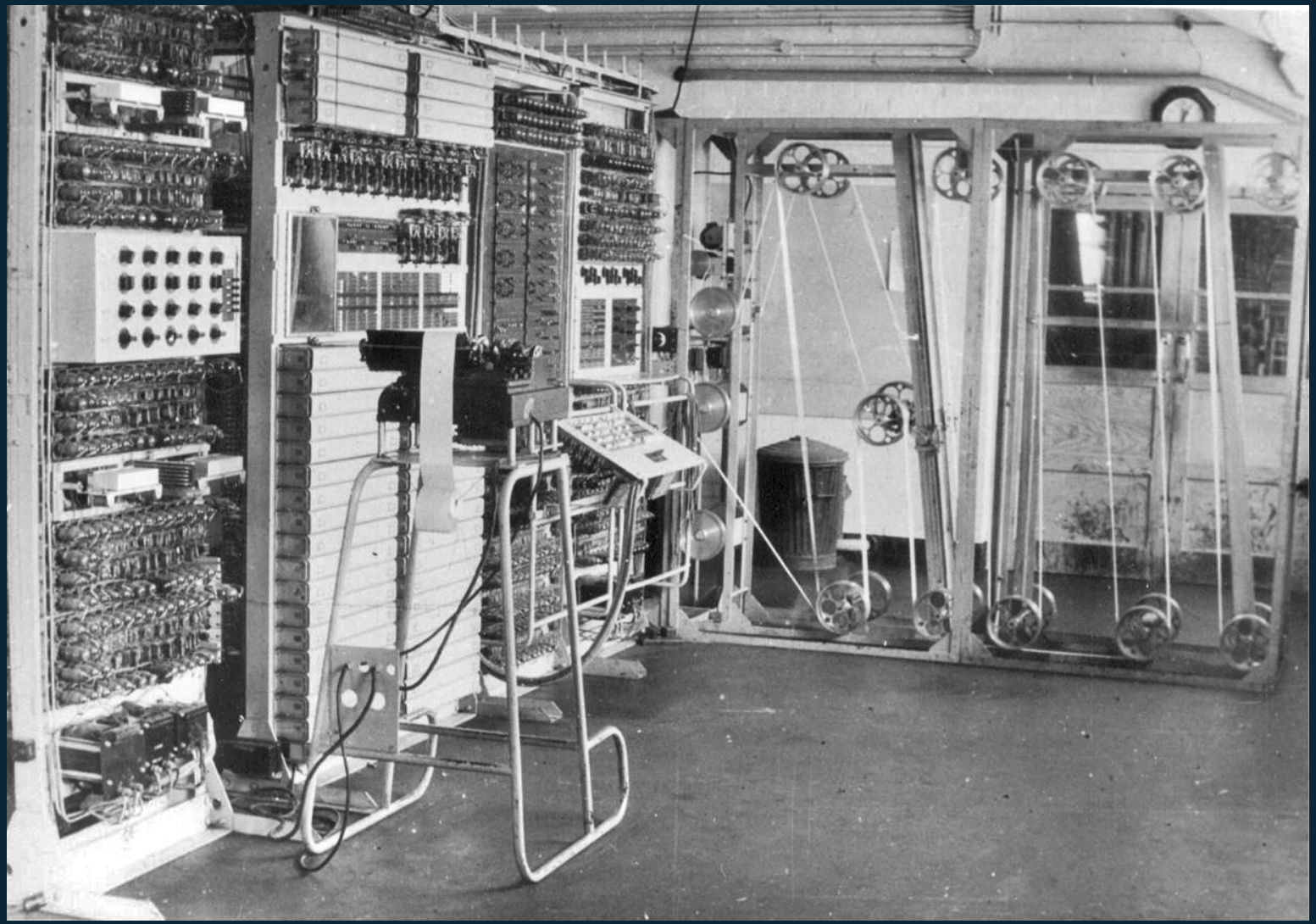
Bombe

Tunny



Lorenz Teleprinter

Colossus



Colossus

Modern Cryptography and How it Effects your Life

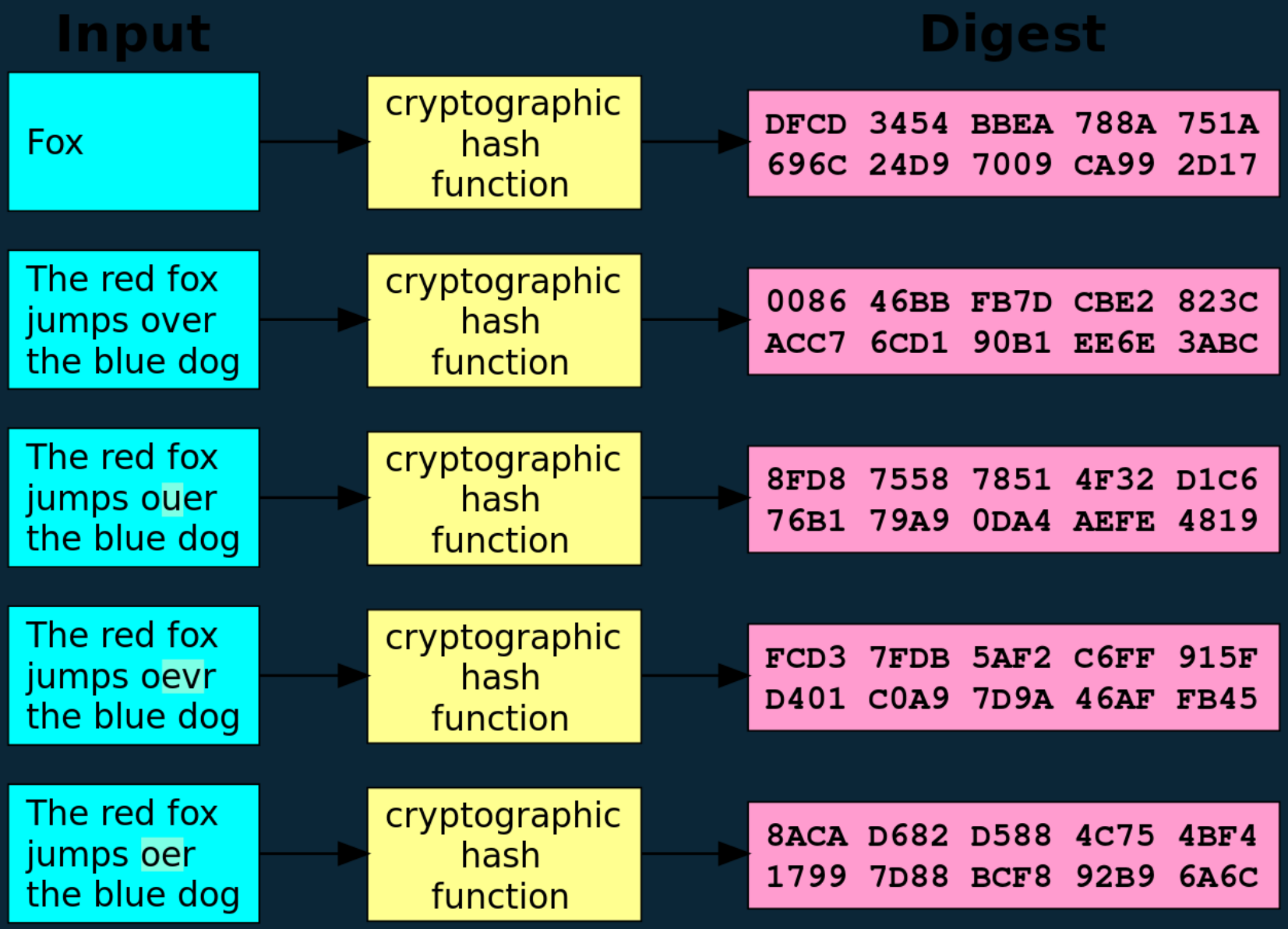
Crypto becomes Maths

- Following 1945 Crypanalysts were winning.
- Ciphers based on symmetric keys were **difficult** but not **hard** to break
- Things changed in the 70's

Hashing

- We use a one way function to turn input into a **hash**
- Small changes to the input can mean large changes to the hashed value
  - MD5, SHA, CRC-32

Hashing


Input
Digest
Fox
cryptographic hash function
DFCD 3454 BBEA 788A 751A
696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog
cryptographic hash function
0086 46BB FB7D CBE2 823C
ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog
cryptographic hash function
8FD8 7558 7851 4F32 D1C6
76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog
cryptographic hash function
FCD3 7FDB 5AF2 C6FF 915F
D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog
cryptographic hash function
8ACA D682 D588 4C75 4BF4
1799 7D88 BCF8 92B9 6A6C

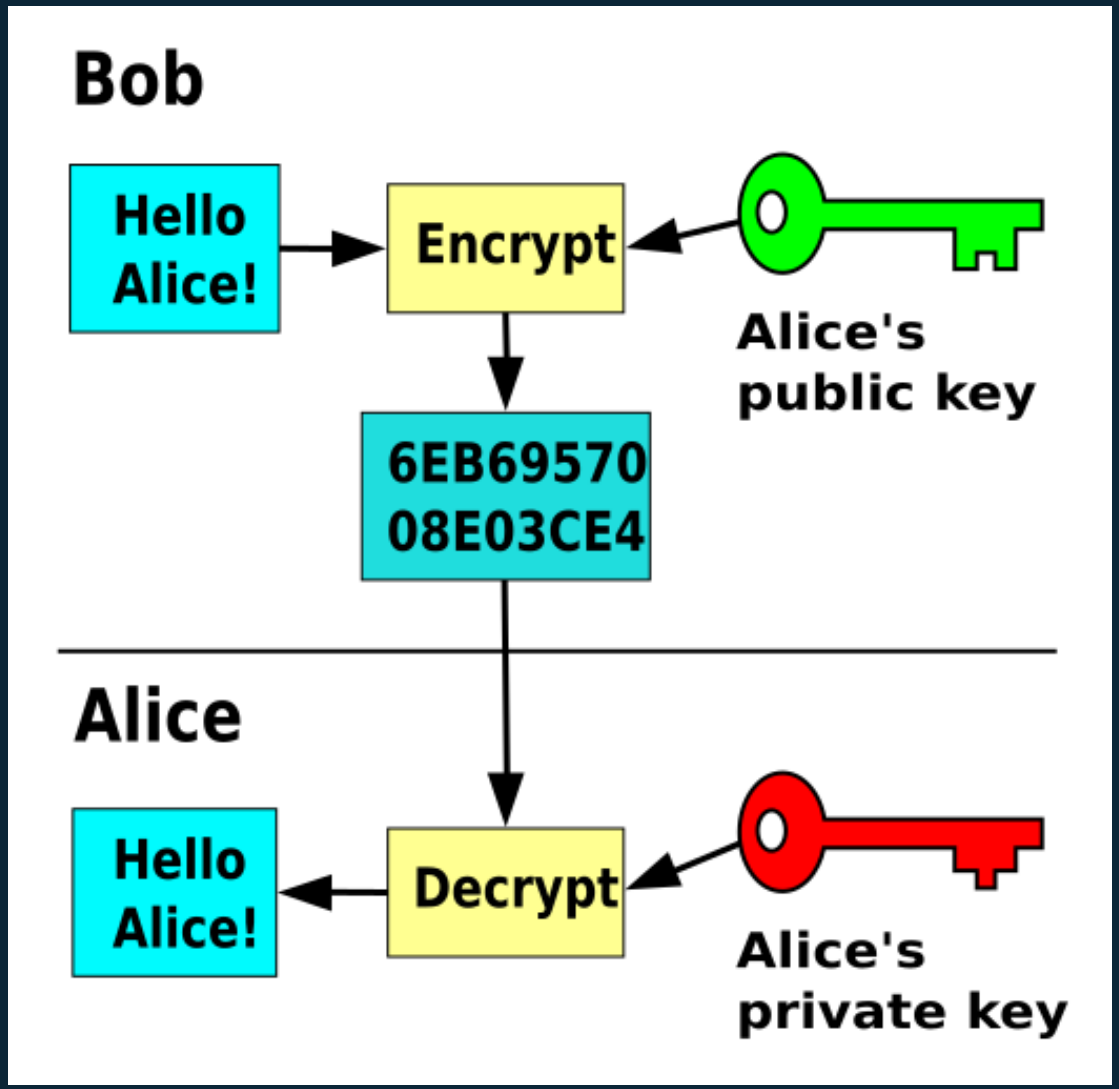
Using Hashes

- Storing Passwords.
  - To avoid pre-calculating the hash, we can add a *salt*
- Confirming Integrity of files
  - The MD5 Sum of this presentation is

Public Key Encryption

- We base our encryption method on:
- - **Public Key** which can be used to encrypt a message to a recipient
  - **Private Key** which is the ONLY way to decrypt a message encoded by the Public key

PKI


Bob
Hello Alice!
Encrypt
Alice's public key
6EB69570 08E03CE4
Alice
Hello Alice!
Decrypt
Alice's private key

PKI: RSA

- First "Public" implementation of PKI was RSA encryption
  - Uses Large Prime numbers as components of the Key
  - "One way" mathematical function for deriving public and private keys
- Even if we know the public part, we need to know the two numbers used to generate it.
  - $33 == 11 \times 3$
  - $259854853 == X? \times Y?$

Breaking RSA

- Depends on the Key length.
  - Exponential curve based on key length.
  - For every Bit added we double the length of time
- Its not Impossible to break, but computationally infeasible

Public Key Infrastructure

- How do we the public key we use to encrypt?
  - I want to send James a secret message, how do I know it's HIS key?
- Certificate Authorities (CA) give us some way of trusting this information
  - We can then check the public key against the CA to confirm identity.

Encrypted Web Pages (HTTPS/ SSL)

- Encrypting the communication between our web browser and the server
  - Online shopping / banking needs to make use of this
  - Any data sent to and from the server is encrypted

Encrypted Web Pages

- An encrypted website has a public key and certificate.
- Public key is used to encrypt data
- Additionally, the certificate is checked. If it is suspicious we get a warning.
- Shpould we get a warning or should it be automatically blocked?
  - Why may a certificate be incorrect.
  - Time Expired etc. Self signed

Encrypted Web Pages: Downsides

- HTTPS is a Really Good Thing (TM). It should be there by default
- But If I can setup a certificate easily, so can the bad guys.
  - about 2/3 of Phishing sites are SSL.
- The Data is secure, and the server it is going to is the one registed
- However, is the site itself legitimate. Can the public CA's check this?

End-to-End Encryption

- Web based communication is still **Client - Server**
  - The Middle man could still read our messages
- Messages are encrypted with each person in the conversations Public Key.
  - Application is responsible for forwarding content, and managing key exchange

Evil Encryption:

- Unfortunately Encryption isn't all for good.
  - Recent(ish) attacks encrypt a victims files
  - Pay a ransom to get the files decrypted
  - Almost impossible to restore the data without the private key
- All based on the Public Key encryption
- Bad guys encrypt the data on your system using their public key.
- Only the private key can get it back
- Some AV companies are publishing details of Private keys as they become known.

Thank You

Please get in touch if you would like to comment, learn more about our courses, or get involved with the Institute Of Coding Coventry University.

- Deepak Farmah: **E.** DFarmah@cueltd.co.uk | **T.** 07392 096215
- Louise Phipps: **E.** LPhipps@cueltd@cueltd.co.uk | **T.** 07392 096318

Please complete the post webinar survey:

https://tinyurl.com/IoC-Webinars-May