Science, Technology, Engineering & Maths (STEM)

Mr Bateson

ROYAL AIR FORCE

air cadets
the next generation

Brief Introduction

- MEng Electronic Engineering, University of York, 2001-05
- RAF Engineering Officer, 2006-11
- Cybersecurity Consultant, PwC and NCC Group, 2011-16
- Head of Cybersecurity, McLaren, 2016-20
- Head of Information Security, Slaughter and May, 2020-now



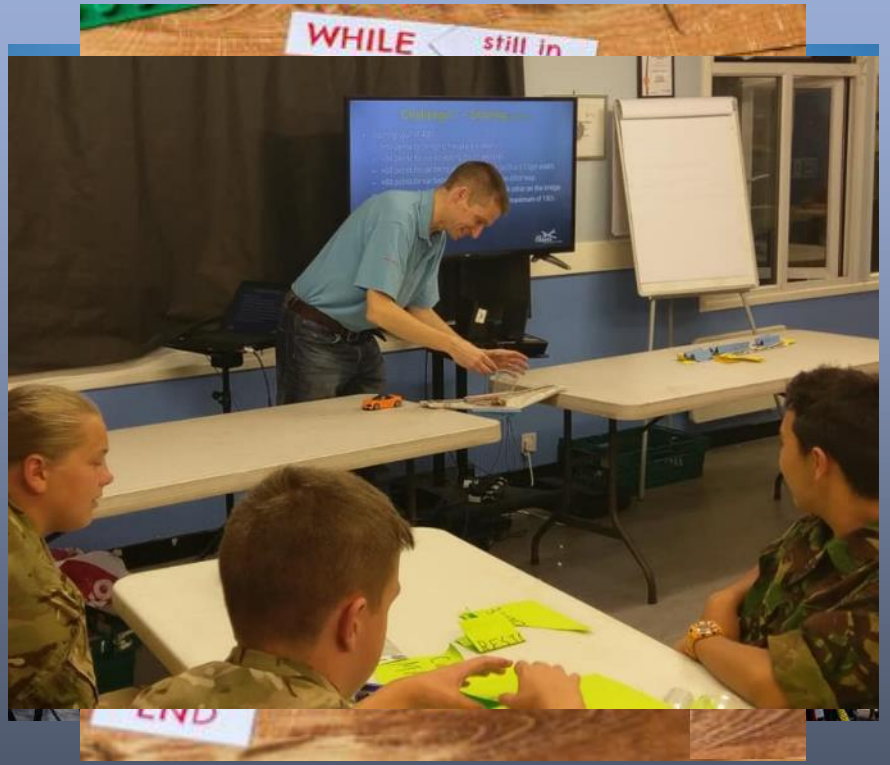



ROYAL AIR FORCE

air cadets
the next generation

Previous STEM Sessions

1. Emerging technologies.
2. Space.
3. Radar and Stealth.
4. Disaster relief.
5. Introduction to programming.
6. Bridge and crane building.



ROYAL AIR FORCE

air cadets
the next generation

This Session



Codes & Codebreaking

- Warm Up Exercise
- Encoding & Decoding
- Ciphers
- Codebreaking

ROYAL AIR FORCE

air cadets the next generation

Before We Start

- These STEM sessions aren't on any exam.
- These slides can be downloaded from www.timbateson.co.uk/rafac/
- No need to write everything down – please focus on taking part.

ROYAL AIR FORCE

air cadets the next generation

Warm-Up Exercise

- Split into 2 teams.
- Each team needs some post-it notes and some marker pens.
- You have 2 minutes (from “go”) to write down lots of:

Team 1

Who might want to **use** codes and when/why

Team 2

Who might want to **break** codes and when/why

- One reason per post-it note.
- It’s team activity – work together!

ROYAL AIR FORCE

air cadets the next generation


Ready?
COUNTDOWN
COUNTDOWN

Warm-Up Exercise

- What did you come up with?

Team 1

Who might want to **use** codes and when/why

Team 2

Who might want to **break** codes and when/why

ROYAL AIR FORCE

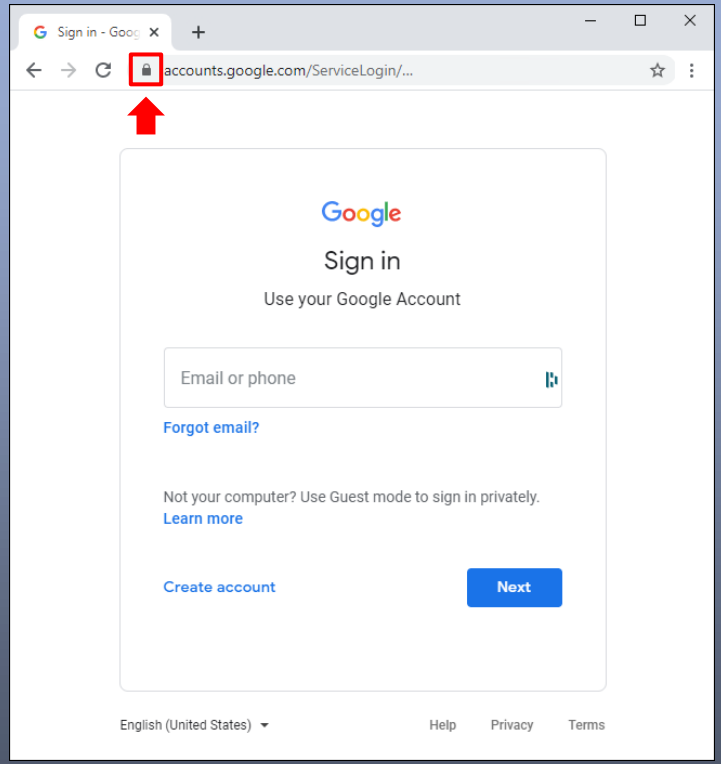
air cadets
the next generation

Who Uses Codes and When?

- Most people in the UK, most days.
  - Anyone who ever uses the internet or a smartphone (probably without even realising it).
- What does the little padlock in your web browser mean?



  - Messages between you and this site are **encrypted** (sent in code).
  - About **80%** of all websites do this.

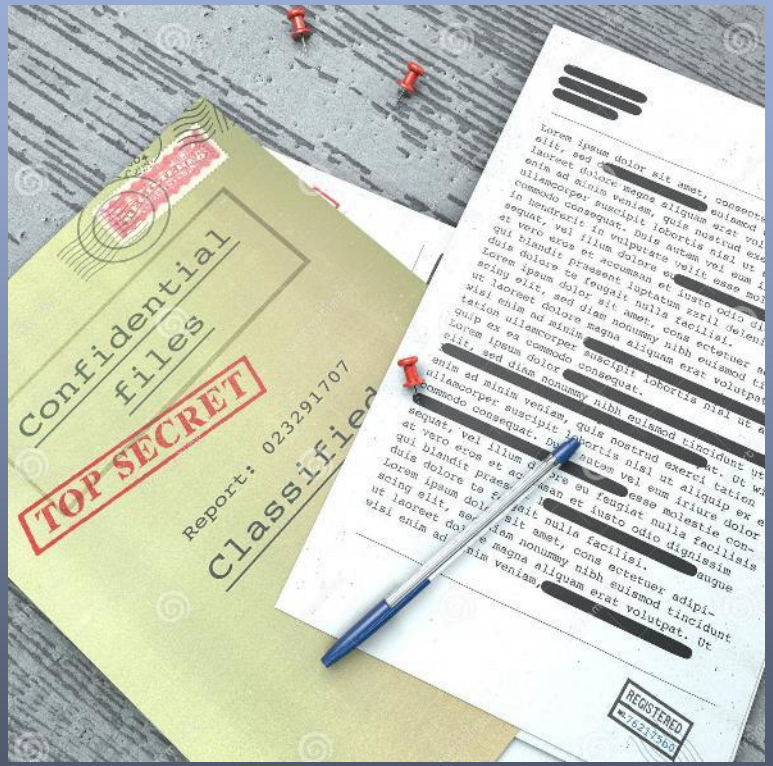


ROYAL AIR FORCE

air cadets
the next generation

Why Use Codes?

- **Confidentiality**
  - Keeping secrets secret.
  - Socially: to keep messages between friends private.
  - In business: to protect things like bank details online.
  - In the military: to keep orders and battle plans secret.



ROYAL AIR FORCE

air cadets
the next generation

Why Use Codes?

- **Authenticity**
  - Proving that a message is genuine.
  - If I receive an encoded message and it decodes correctly…
  - …then the sender is using the right codebook (cipher and keys)…
  - …which means I can probably trust that the message is authentic.
  - How much I trust that depends on how secure the codebook is.



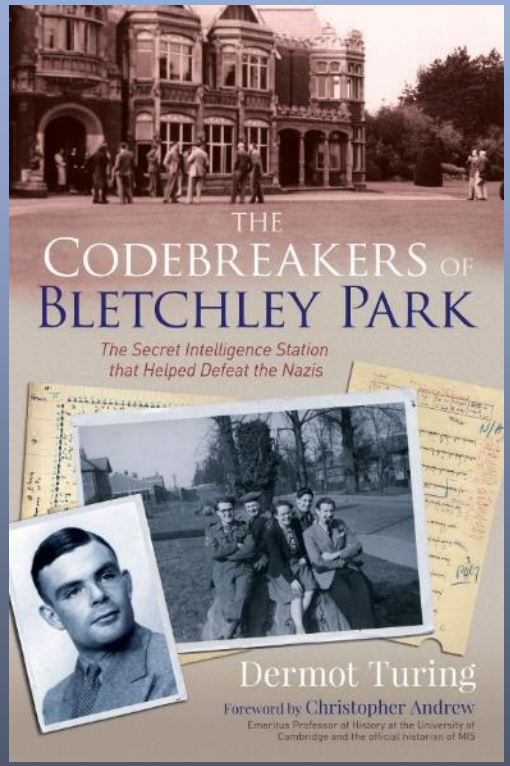
"On the Internet, nobody knows you're a dog."

ROYAL AIR FORCE

air cadets
the next generation

Who Breaks Codes and When?

- **Governments, militaries, intelligence**
  - To find out other countries' plans.
- **Law enforcement**
  - To detect and prevent crimes.
- **Criminals**
  - To steal your passwords or bank details.
- **Mathematicians and researchers**
  - To make better codes.
  - For the challenge.



ROYAL AIR FORCE

air cadets
the next generation

Why Break Codes?

- Breaking an adversary's codes, preferably without them knowing, provides an **advantage**.
  - You can see what they are saying.
  - You might be able to send them fake messages that they believe are real.
  - You might damage their confidence that their messages are private and can be trusted, disrupting their activities.
- Short video.



ROYAL AIR FORCE

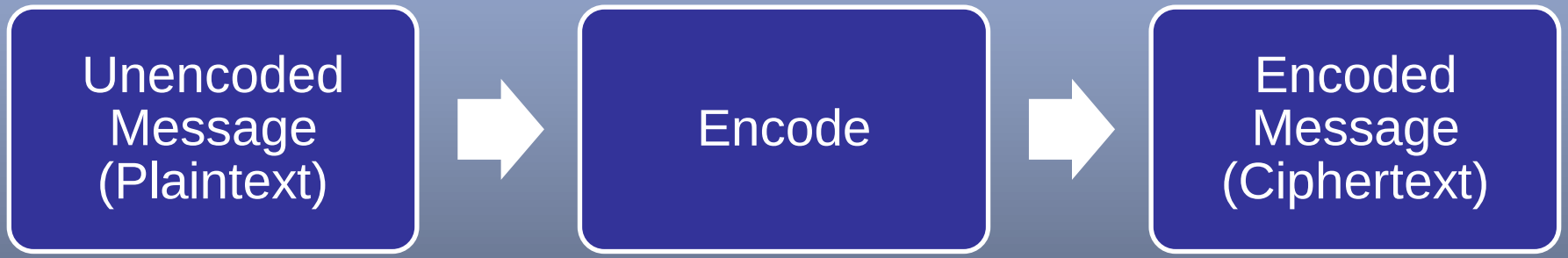
air cadets the next generation

Video 1

Codebreakers (Link)

Encoding & Decoding

- **Encoding** is the process of converting an unencoded message (plaintext) into an encoded message (ciphertext).



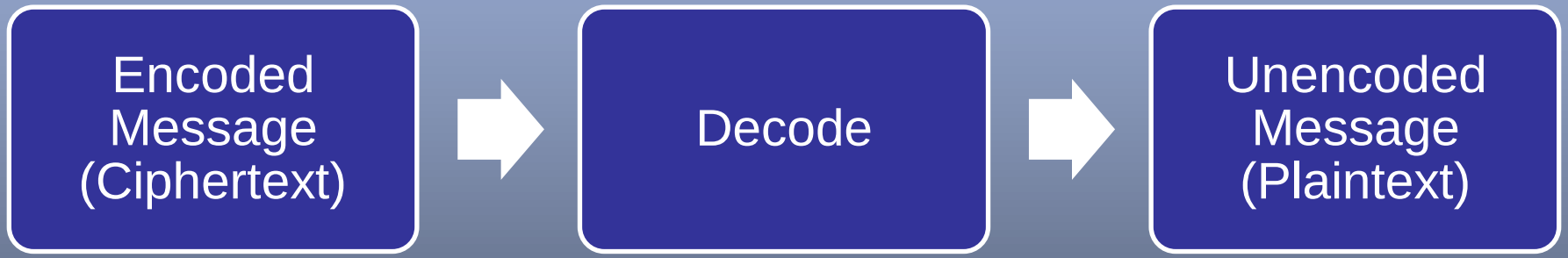
- Plaintext = the unencoded message you start with.
- Ciphertext = the encoded message you end up with.
- Encoding = the process of converting it.

ROYAL AIR FORCE

air cadets
the next generation

Encoding & Decoding

- **Decoding** is the process of converting an encoded message (ciphertext) into an unencoded message (plaintext).



- Ciphertext = the encoded message you start with.
- Plaintext = the unencoded message you end up with.
- Decoding = the process of converting it.

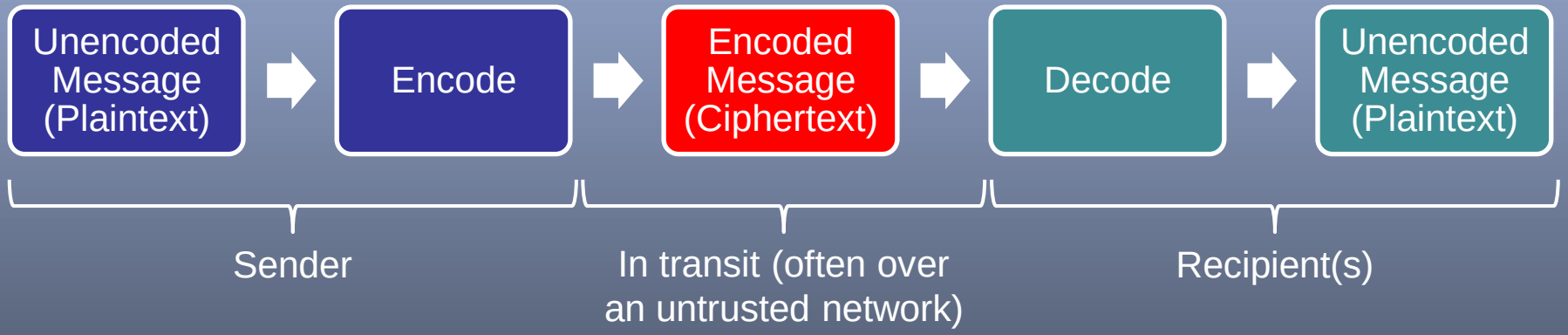
ROYAL AIR FORCE

air cadets
the next generation

Encoding & Decoding

- The whole process:





ROYAL AIR FORCE
air cadets the next generation

Ciphers

- The specific conversion rules that you follow when encoding and decoding a message is the **cipher** (or cypher).
- Sometimes the cipher takes the form of a **codebook**.

- We're going to try out 3 different ciphers today:
  1. The **Shift** Cipher.
  2. The **Substitution** Cipher.
  3. The **Rotating** Cipher.

ROYAL AIR FORCE

air cadets the next generation

The Shift Cipher

- The Shift Cipher is the simplest.
- First used by the Romans – also known as the Caesar Cipher.
- Every letter is shifted up by a fixed number of places.
- For example, shifting up by 3 places (‘scrambler setting 3’):

Plain Alphabet	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
Cipher Alphabet	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

- Easy to encode, but also fairly easy to break.

ROYAL AIR FORCE

air cadets the next generation

The Shift Cipher – Example

- The message “send air support” encodes, using a shift cipher with a scrambler setting of +3, as:

Plaintext Message	S	E	N	D		A	I	R		S	U	P	P	O	R	T
Encoded Message	V	H	Q	G		D	L	U		V	X	S	S	R	U	W

- Scrambler setting +3 conversion table:

Plain Alphabet	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
Cipher Alphabet	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

ROYAL AIR FORCE

air cadets the next generation

The Shift Cipher – Exercise 1

- Encode the following message, using a shift cipher with a scrambler setting of +10:

Plaintext Message	S	E	N	D		A	I	R		S	U	P	P	O	R	T
Encoded Message	C	O	X	N		K	S	B		C	E	Z	Z	Y	B	D

- Scrambler setting +10 conversion table:

Plain Alphabet	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
Cipher Alphabet	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

ROYAL AIR FORCE

air cadets the next generation

The Shift Cipher – Exercise 2

- Decode the following message, using a shift cipher with a scrambler setting of +17:

Encoded Message	J	V	E	U		R	D	S	L	C	R	E	T	V
Plaintext Message	S	E	N	D		A	M	B	U	L	A	N	C	E

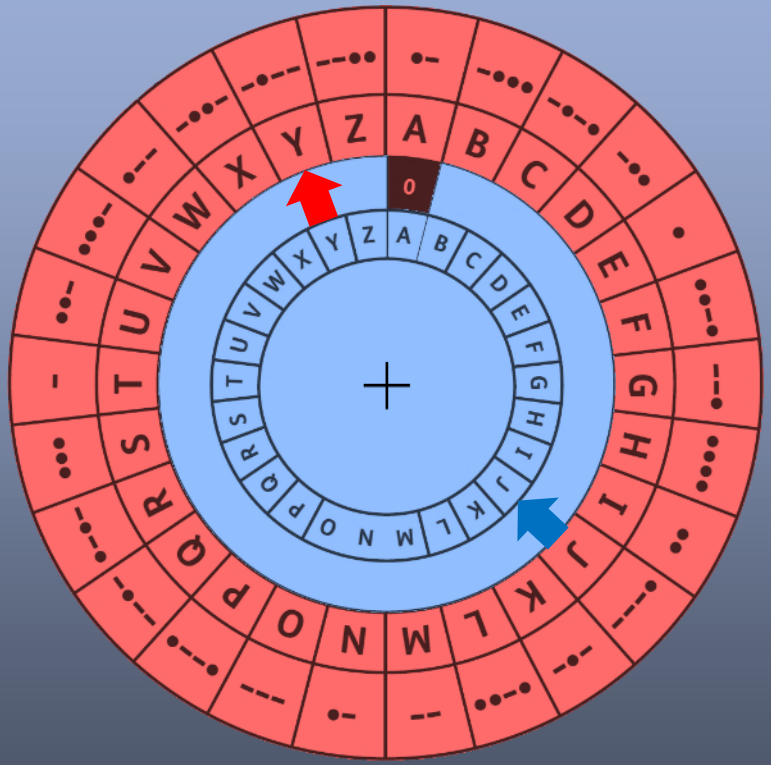
- Scrambler setting +17 conversion table:

Plain Alphabet	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
Cipher Alphabet	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

ROYAL AIR FORCE

air cadets the next generation

Using a Code Wheel



- A ‘code wheel’ can speed up encoding and decoding.
  - The encoded letters are on the outer dial.
  - The unencoded letters are on the inner dial.
  - Turn the inner dial to select the right scrambler setting.
  - Read inside-out to encode.
  - Read outside-in to decode.

ROYAL AIR FORCE

air cadets the next generation

The Shift Cipher – Exercise 3

- Using a code wheel, decode the following message, using a shift cipher with a scrambler setting of +5:

Encoded Message	N	X		N	Y		G	W	J	F	P		D	J	Y
Plaintext Message	I	S		I	T		B	R	E	A	K		Y	E	T

ROYAL AIR FORCE

air cadets the next generation

The Substitution Cipher

- The Substitution Cipher is the next simplest.
- Every letter is swapped (substituted) for another letter.
  - The same letter substitution is made each time.
  - The cipher alphabet isn't necessarily in alphabetical order.
- You need the right codebook to encode and decode.
- For example, using the key phrase 'Royal Air Force':

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

ROYAL AIR FORCE

air cadets the next generation

The Substitution Cipher – Exercise 4

- Encode the following message, using the ‘Royal Air Force’ substitution cipher:

Plaintext Message	S	E	N	D		A	I	R		S	U	P	P	O	R	T
Encoded Message	U	L	M	A		R	E	T		U	W	Q	Q	P	T	V

- Conversion table for key phrase ‘Royal Air Force’:

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

ROYAL AIR FORCE

air cadets the next generation

The Substitution Cipher – Exercise 5

- Decode the following message, using the ‘Royal Air Force’ substitution cipher:

Encoded Message	U	L	M	A		K	P	T	L		V	L	R
Plaintext Message	S	E	N	D		M	O	R	E		T	E	A

- Conversion table for key phrase ‘Royal Air Force’:

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

ROYAL AIR FORCE

air cadets the next generation

The Rotating Cipher

- The Rotating Cipher is more complex.
- The letter substitution used changes over time.
- For example, using a starting scrambler setting of +2:

Plaintext Message	S	E	N	D		A	I	R		S	U	P	P	O	R	T
Scrambler Setting	+2	+3	+4	+5		+6	+7	+8		+9	+10	+11	+12	+13	+14	+15
Encoded Message	U	H	R	I		G	P	Z		B	E	A	B	B	F	I

- The first S becomes U (+2); the second S becomes B (+9).
- Both ends need to agree the scrambler setting to start on.

ROYAL AIR FORCE

air cadets the next generation

The Rotating Cipher – Exercise 6

- Encode the following message, using a rotating cipher with a starting scrambler setting of +9:

Plaintext Message	A	T	T	A	C	K		A	T		D	A	W	N
Scrambler Setting	+9	+10	+11	+12	+13	+14		+15	+16		+17	+18	+19	+20
Encoded Message	J	D	E	M	P	Y		P	J		U	S	P	H

- A code wheel really helps here!

ROYAL AIR FORCE

air cadets the next generation

The Rotating Cipher – Exercise 7

- Decode the following message, using a rotating cipher with a starting scrambler setting of +17:

Encoded Message	J	W	G	X		W	E	P	A	T	I	U	U
Scrambler Setting	+17	+18	+19	+20		+21	+22	+23	+24	+25	+0	+1	+2
Plaintext Message	S	E	N	D		B	I	S	C	U	I	T	S

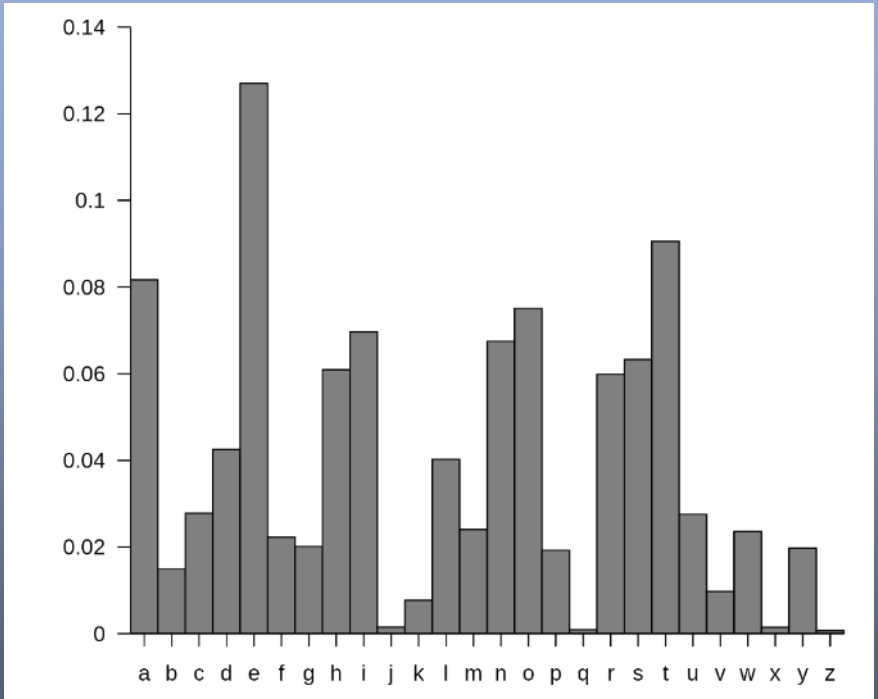
- A code wheel really helps here!

ROYAL AIR FORCE

air cadets the next generation

Codebreaking – Frequency Analysis

- Some letters are used more often than others in English.
  - e.g. “e”, “t”, “a”, “o” and “i”.
- Might guess that whatever letter appears most in a piece of ciphertext might decode to one of these.
  - Can test that assumption and work from there.



Frequency with which each letter appears in English writing

ROYAL AIR FORCE

air cadets the next generation

Codebreaking – Frequency Analysis

- Some words also appear more frequently than others.
- Might guess that:
  - A one letter word decodes to “a” or “i”.
  - A 2 letter word decodes to “of”, “to”, “in”, “it” or “is”.
  - A 3 letter word decodes to “the”, “was” or “for”.
- Can test and develop.

1. the	26. had	51. no	76. just
2. of	27. his	52. said	77. may
3. and	28. they	53. who	78. these
4. to	29. from	54. more	79. new
5. a	30. she	55. about	80. also
6. in	31. which	56. up	81. people
7. that	32. or	57. them	82. any
8. it	33. we	58. some	83. know
9. is	34. an	59. could	84. very
10. was	35. there	60. him	85. see
11. I	36. her	61. into	86. first
12. for	37. were	62. its	87. well
13. on	38. one	63. then	88. after
14. you	39. do	64. two	89. should
15. he	40. been	65. out	90. than
16. be	41. all	66. time	91. where
17. with	42. their	67. like	92. back
18. as	43. has	68. only	93. how
19. by	44. would	69. my	94. get
20. at	45. will	70. did	95. most
21. have	46. what	71. other	96. way
22. are	47. if	72. me	97. down
23. this	48. can	73. your	98. our
24. not	49. when	74. now	99. made
25. but	50. so	75. over	100. got

The 100 most common English words

ROYAL AIR FORCE

air cadets the next generation

Codebreaking – Exercise 8

- Decode the following intercepted enemy communication:

Encoded Message	Y	Q	Q	F		Y	Q		M	F		Z	A	A	Z
Plaintext Message	M	E	E	T		M	E		A	T		N	O	O	N

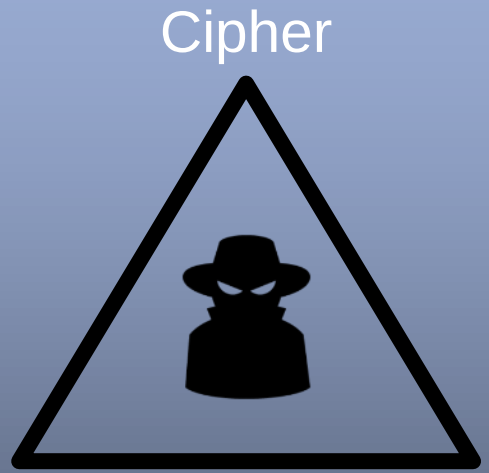
- Reminder:
  - “e”, “t”, “a”, “o” and “i” are the most common letters in English.

- What cipher is the enemy using?
  - A Shift Cipher with a scrambler setting of +12.

ROYAL AIR FORCE

air cadets the next generation

Codebreaking – Known Plaintext Attack



- Given any 2 of these things, you can work out the third.

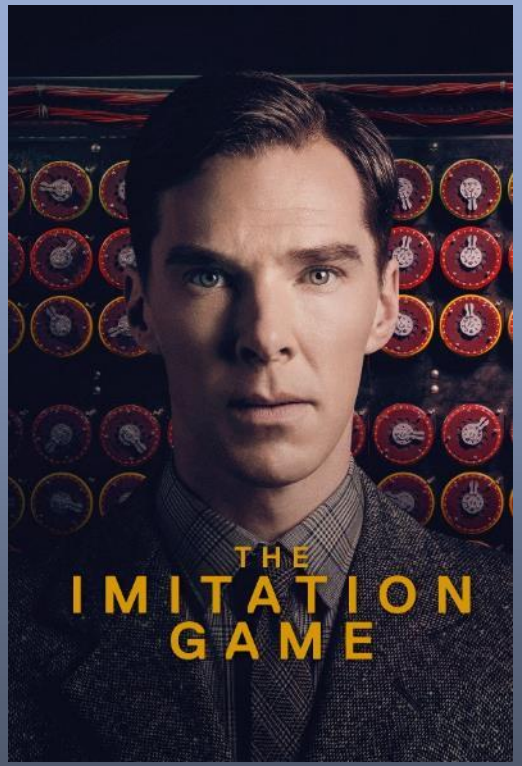
- Only secure if an attacker only knows at most one thing (usually the ciphertext).
- If I intercept ciphertext between 2 people, and then observe them meeting, then I could guess that the meeting location was in the plaintext somewhere.
  - A **known plaintext attack**.

ROYAL AIR FORCE

air cadets the next generation

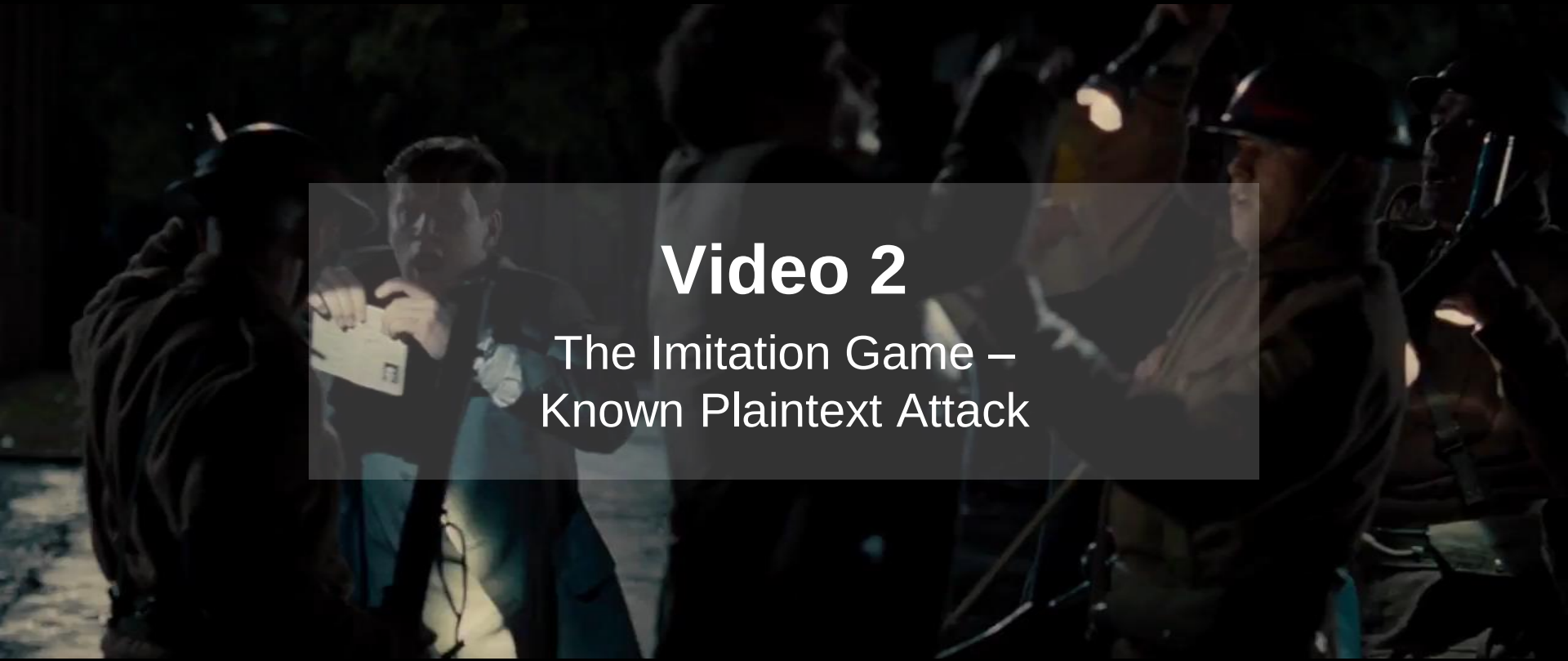
Codebreaking – Known Plaintext Attack

- Short video clip from the film “The Imitation Game”.
  - About Bletchley Park cracking German Enigma codes during World War 2.
  - Focuses on Alan Turing, who invented the first computer (“Christopher”) to crack Enigma.
  - Features a good example of a known plaintext attack.



ROYAL AIR FORCE

air cadets
the next generation



Video 2

The Imitation Game –
Known Plaintext Attack

Codebreaking – Exercise 9

- Decode the following intercepted enemy communication:

Encoded Message	V	J	J	P		G	P		P	B	J		Z	Q	F	J	Z
Plaintext Message	M	E	E	T		A	T		T	H	E		R	I	V	E	R

- After receiving the message, we followed the enemy to a river.
- What do we know about the codebook the enemy is using?

Plain Alphabet	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
Cipher Alphabet	G				J			B	Q				V					Z		P		F				

ROYAL AIR FORCE

air cadets the next generation

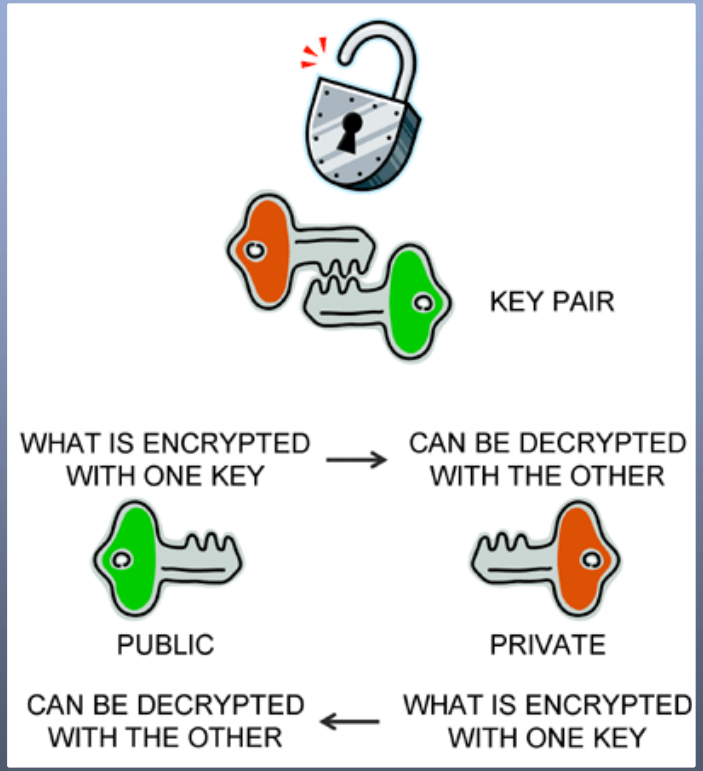
Symmetric & Asymmetric Encryption

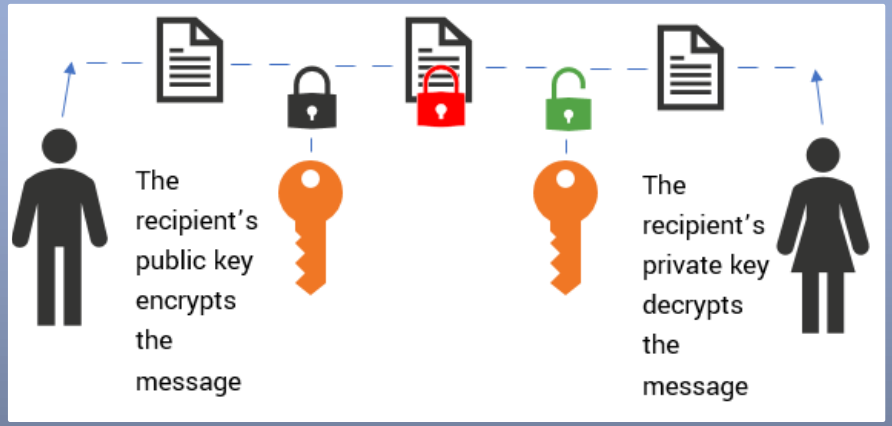
- Everything we've looked at today is **symmetric** encryption.
  - 'Symmetric' because whatever cipher is used to encode a message, the same cipher is used to decode it.
  - The processes of encoding and decoding mirror each other.
- Not always easy to agree the cipher securely in the first place!
- There is a way to overcome this – **asymmetric** encryption.
  - 'Asymmetric' as the sender and receiver use **different** ciphers.
  - This is the technology that secure webpages use.
  - How it works is complicated, but in overview…

ROYAL AIR FORCE

air cadets the next generation

Asymmetric Encryption





- Very **easy** to get the public key from the private key.
- Very **hard** to get the private key from the public key.

ROYAL AIR FORCE

air cadets
the next generation

Summary

- Discussed who uses codes, when and why.
- Discussed who tries to break codes, when and why.
- Practiced encoding and decoding messages using 3 ciphers:
  - Shift Cipher.
  - Substitution Cipher.
  - Rotating Cipher.
- Discussed and had a go at some codebreaking techniques.
  - Frequency analysis and known plaintext attack.
- Touched on asymmetric encryption.

ROYAL AIR FORCE

air cadets the next generation

Any Questions?

(Feel free to ask in private if you prefer)

ROYAL AIR FORCE

air cadets
the next generation