Cryptography Introduction

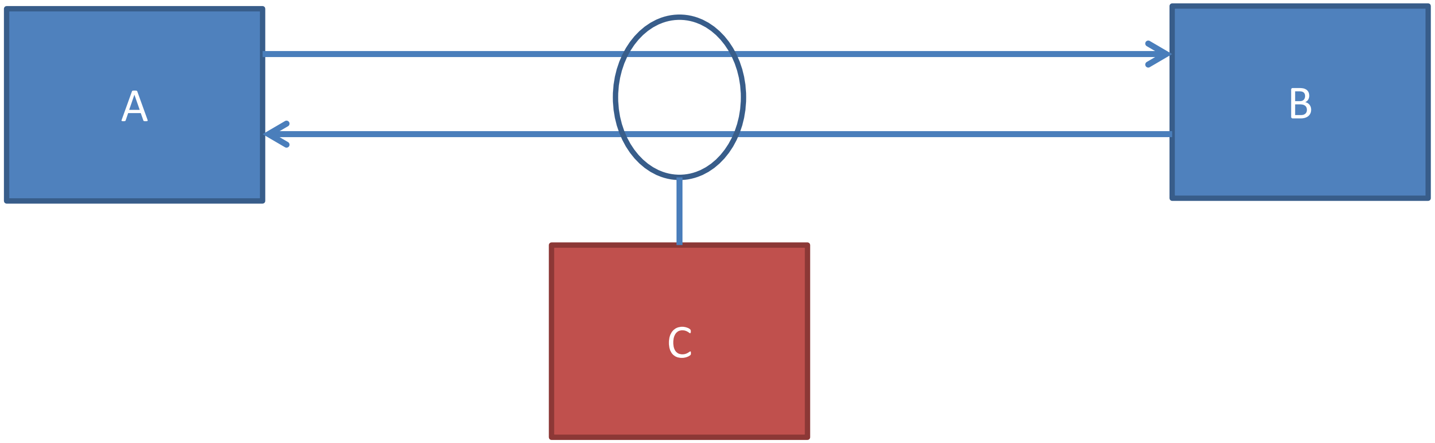
Jack Bradbrook

Topics

- What is Cryptography?
- Keys and Ciphers
- The Caesar Cipher
- Frequency Analysis
- The Enigma Cipher
- The one time Pad/ What is perfect Encryption?
- The Nature of Randomness in relation to Cryptography
- Computers and pseudo random numbers.

What is Cryptography

- Derived from ancient greek word “kryptós” meaning “Hidden Secret”
- Allows communication between two parties without a third party intercepting and understanding or manipulating that information.



Significance of Cryptography

- Cryptography underpins the modern world.
  - Human communication.
    - Personal details
    - Military intelligence
  - Identity verification
    - Digital Applications
    - Online Banking / financial transactions
- Cryptography is Old!
  - Some techniques date back thousands of years

How it works?

- A regular message known as ***Plain Text*** PT, when transported over some physical medium is vulnerable to interception from a third party.

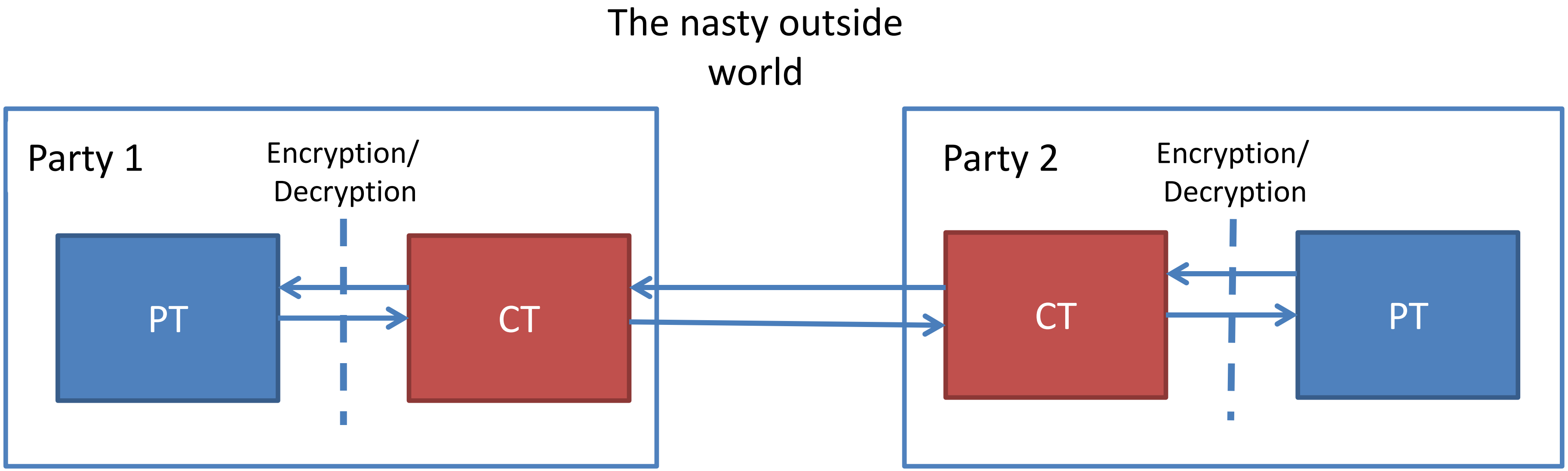
e.g. “The Enemy Are Heading South”,

- To prevent this the message is sent as a ***Cypher Text*** CT, this cannot be read without first converting the cypher text back to the plain text.

e.g. “Vjg Gpgoa Ctg Jgcfkpi Uqwvj”

Encrypting/ Decrypting

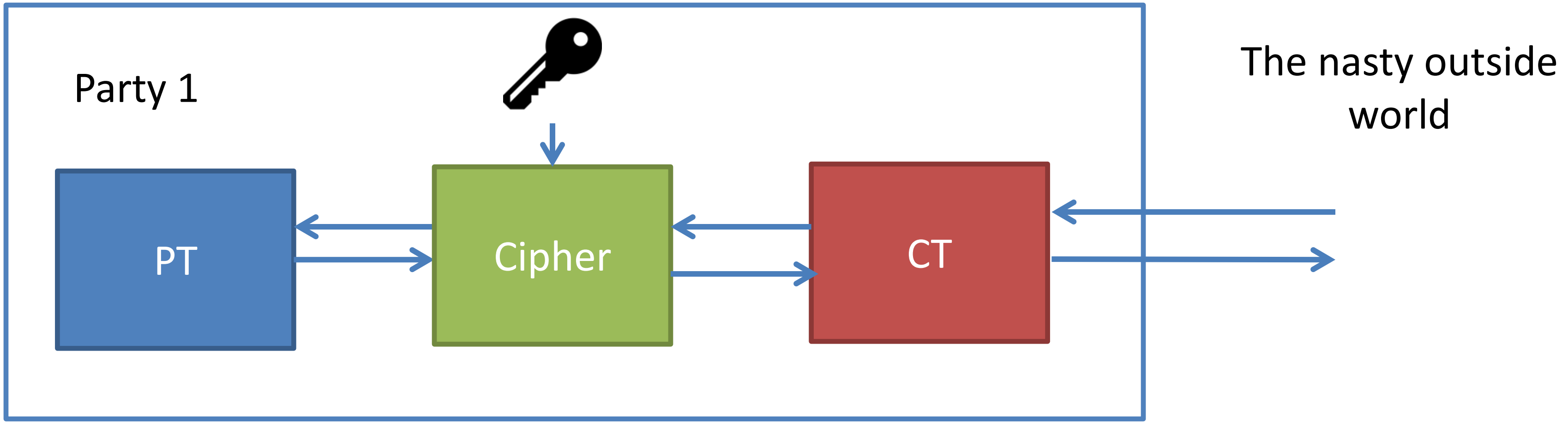
- The process of converting PT to CT is ***Encryption***
- The process of converting CT to PT is ***Decryption***
- A ***Cipher*** is a pair of algorithms, a series of steps that are applied which can convert PT -> CT or CT -> PT



How does a Cipher work?

- For the cipher to convert PT to CT it uses an additional piece of information known as the ***key***

- Once CT exists knowing the inverse of the key will convert CT back to PT



The Caesar Cipher

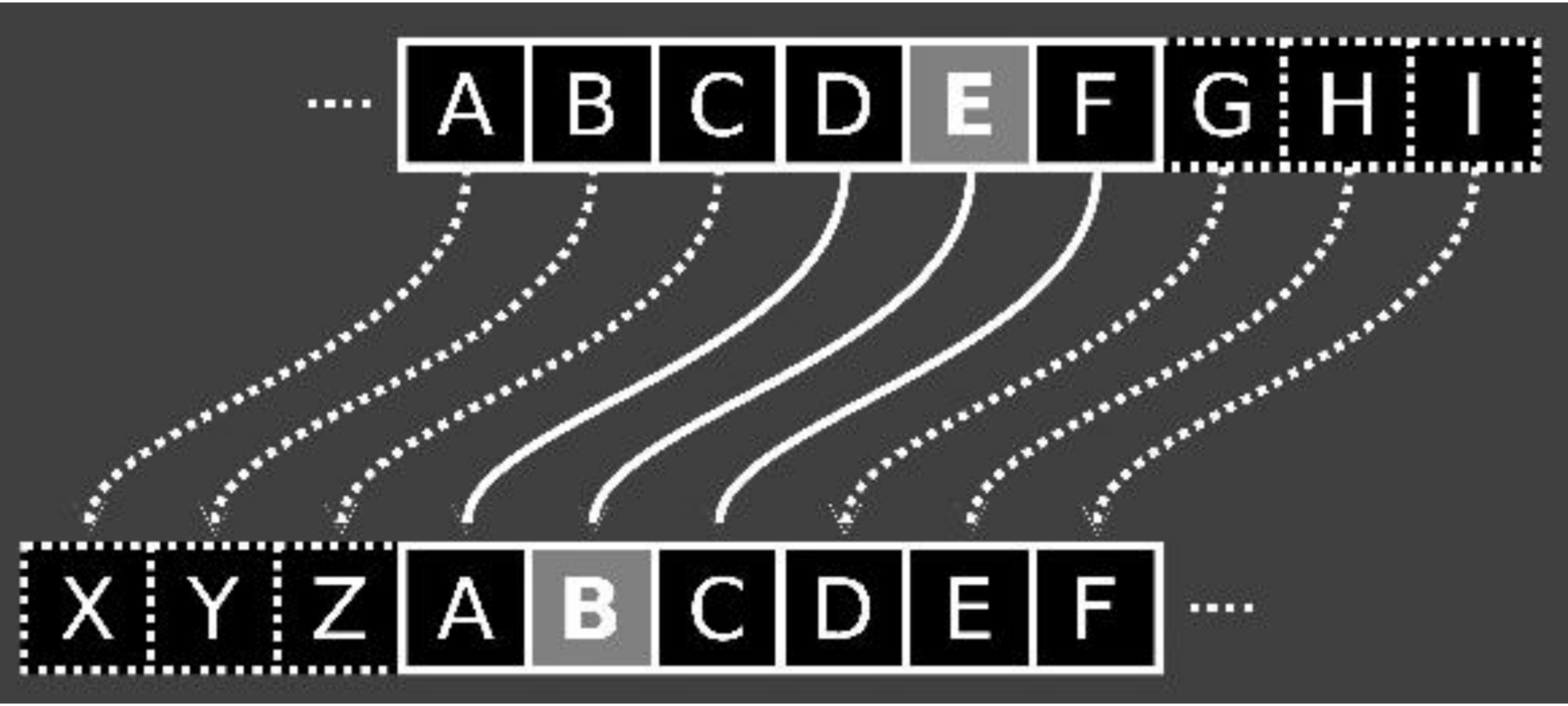
- Probably the most basic example of a cipher

- Used by Julius Caesar to issue commands to generals during his invasion of Gaul

- Works by shifting **all the characters** in the plaintext along in the alphabet by some amount *x*

- The key is the number of

characters by which to shift the message


A
B
C
D
E
F
G
H
I
X
Y
Z
A
B
C
D
E
F

Caesar cipher example

- Plain Text: “The Enemy Are Heading South”,
- Key (x): 2

- Cipher (encrypt): shift each character **right** along the alphabet by x (The Key)

…

- Resulting Cipher Text: “Vjg Gpgoa Ctg Jgcfkpi Uqwvj”

…

- Cipher (decrypt): shift each character **left** along the alphabet by x

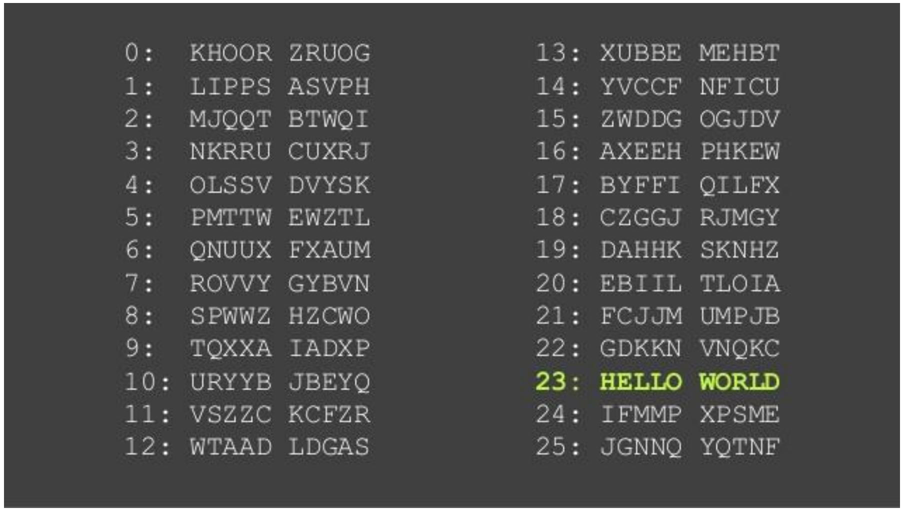
… *(process is undone)*

- Plain Text: “The Enemy Are Heading South”,

What’s the problem with this?

- If the method is revealed to a third party then the message can be uncovered by trial and error, there are 26 possible translations of the CT, into the PT, try each shift in turn without any special strategy, this is known as ***Brute Force Search***.

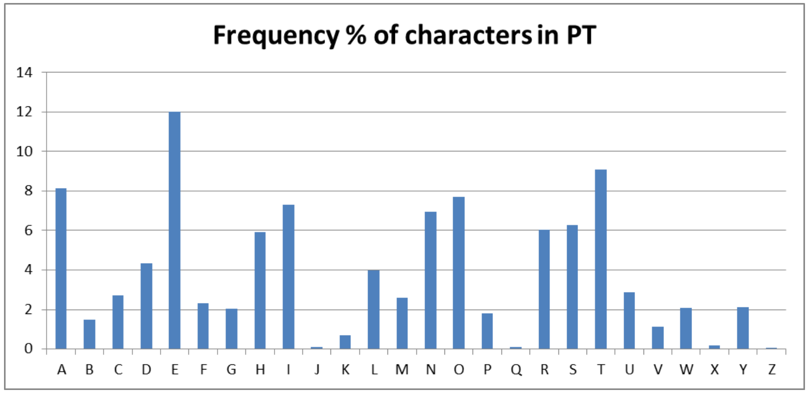
- Common patterns exist in both the PT and the CT which expose the key.

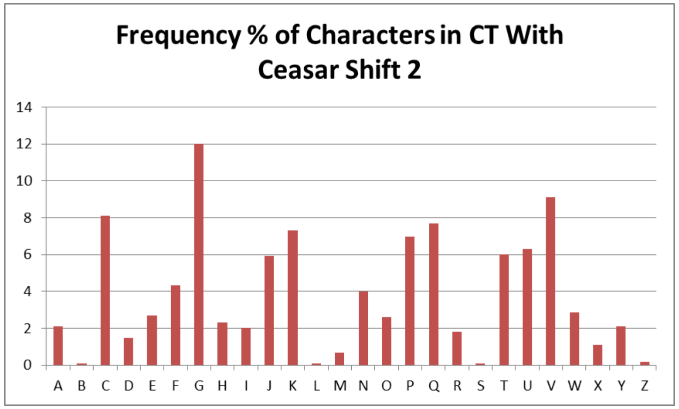


```
0:   KHOOR ZRUOG          13: XUBBE MEHBT
1:   LIPPS ASVPH          14: YVCCF NFICU
2:   MJQQT BTWQI          15: ZWDDG OGJDV
3:   NKRRU CUXRJ          16: AXEEH PHKEW
4:   OLSSV DVYSK          17: BYFFI QILFX
5:   PMTTW EWZTL          18: CZGGJ RJMGY
6:   QNUUX FXAUM          19: DAHHK SKNHZ
7:   ROVVY GYBVN          20: EBIIL TLOIA
8:   SPWWZ HZCWO          21: FCJJM UMPJB
9:   TQXXA IADXP          22: GDKKN VNQKC
10:  URYYB JBEYQ          23: HELLO WORLD
11:  VSZZC KCFZR          24: IFMMP XPSME
12:  WTAAD LDGAS          25: JGNNQ YQTNF
```

Frequency analysis

- Problem: The English language makes greater use of some characters than others, therefore Caesar shift leaves a close correlation between the PT and CT



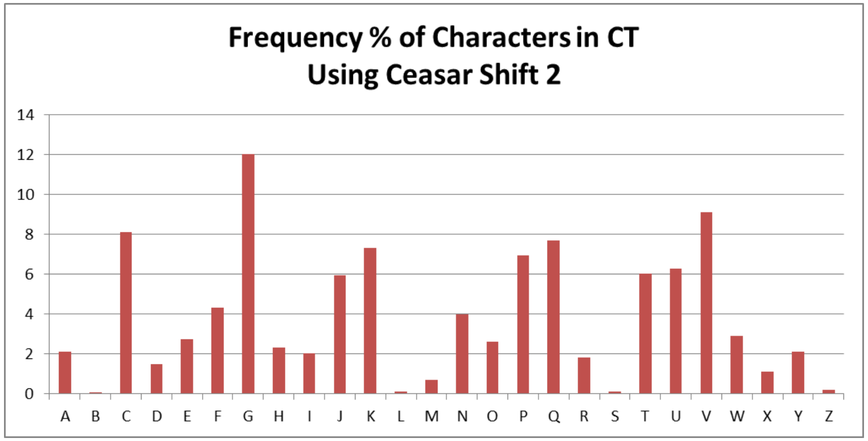


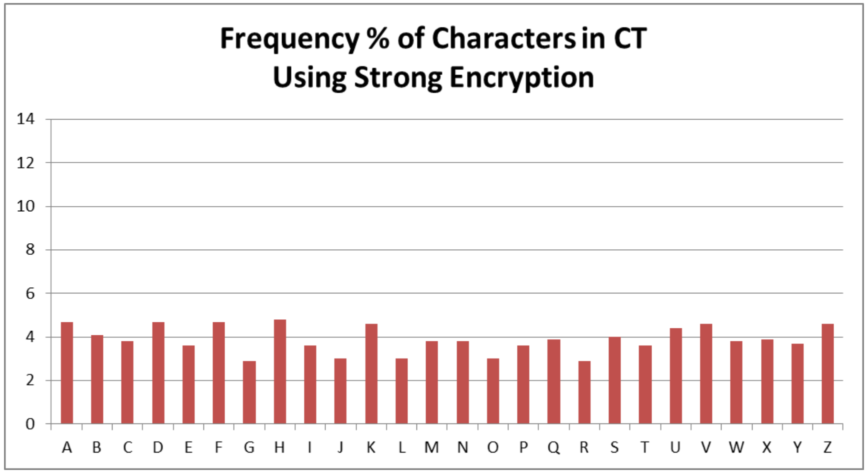
Strong vs Weak Ciphers

- A strong cipher will make the CT appear completely random to an interceptor i.e. there is nothing that can be observed in it which is useful for deducing how it was originally generated from some PT.

- Reoccurring patterns in the CT or correlations between the CT and the PT reveal information about the key and the design of the Cipher to an interceptor.

- The process of understanding the nature of the cipher or key from this information is known as "Cryptanalysis".

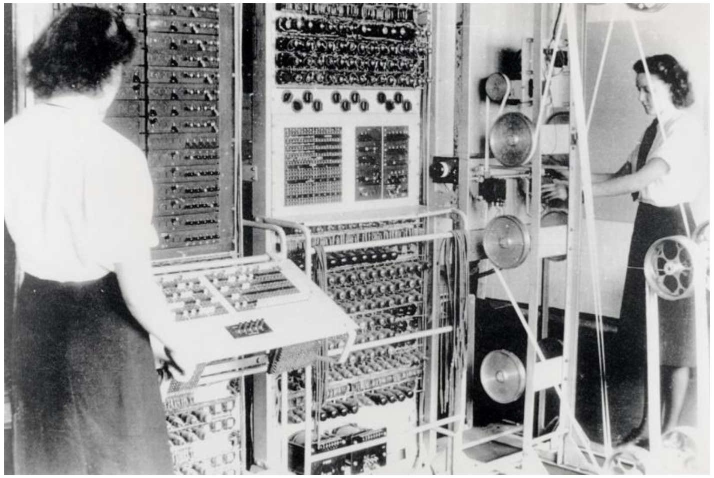




Cryptanalysis (code breaking)

Bletchley Park during WW2 huge operation to perform Cryptanalysis of the German Enigma machines, Used to encode messages between German command and ground forces and U boats from a distance.

The work later lead on to the development of Colossus the first world's first programmable, electronic, digital computer

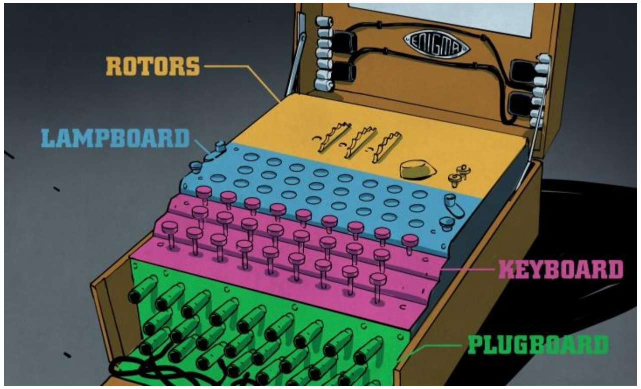


Example 2: The Enigma Machine

- A electro mechanical machine which performs the encryption and decryption operations for a human. An absolute icon of cryptography!
- Comprised of:
  - A keyboard, allows operator to issue an input character
  - A lamp board, allows the machine to indicate an encrypted or decrypted character corresponding to the key pressed by the operator

    CT char -> PT char, or

    PT char -> CT char
  - Rotors, wheels allow the machine to perform substitutions of one character to another.
  - The plug board, allows operator to add an additional substitution themselves.



Enigma Rotor wheels

- Three wheels are used in the machine out of a possible 5 wheels that can be selected

- The wheels have the numbers 1-26 on their side, each number is associated with another number where the signal is outputted having gone through the wheel e.g. the signal comes into the first wheel at position 16 which corresponds to position 3 so the second wheel will receive an input signal where position 3 on wheel one is connected to wheel two.

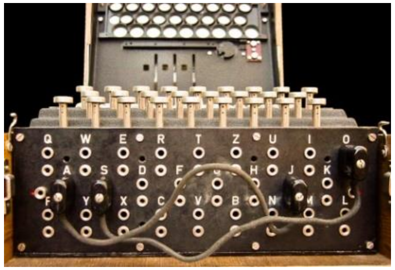
- The operator can set the initial position of the numbers on the wheels.

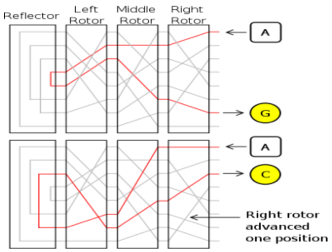
- Each wheel therefore performs one individual character substitution, this substitution is physically built into the wiring inside that wheel.

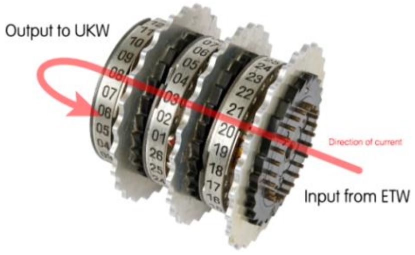
- The output of each substitution is then fed into the next wheel.

- After each substitution the first wheel rotates by one place, after a full rotation the second wheel rotates by one place, similar to a clock, 60 seconds = 1 more minute, 60 minutes = one more hour...

- The output of the final wheel is then substituted again by the operator changing the wiring on the plug board at the front of the machine







Exercise 2:

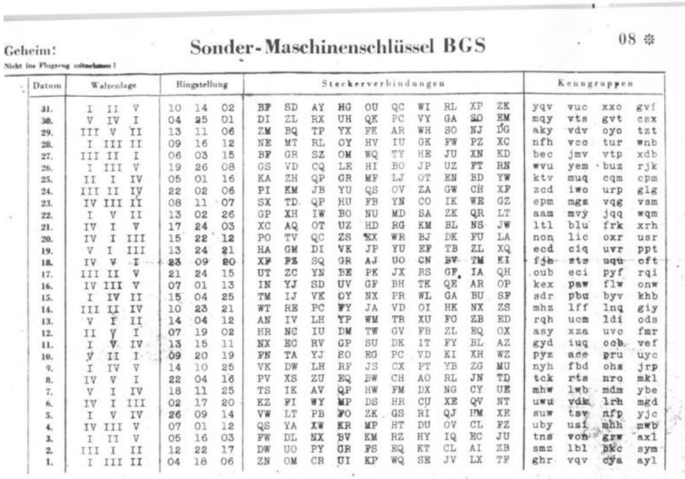
1. What information makes up the key in the enigma system?
   - Hint: think about what information you would need to know to configure the enigma machine to decode a specific message.

2. What aspects of the machine are the Cipher, the Algorithm which transforms the PT to the CT using the key?
   - Hint: think about how the machine actually works once it's been given the key.

The Enigma Key

The enigma key is comprised of:

1. The wheels chosen to put into the machine
2. The starting positions of the wheels
3. The configuration of the plug board



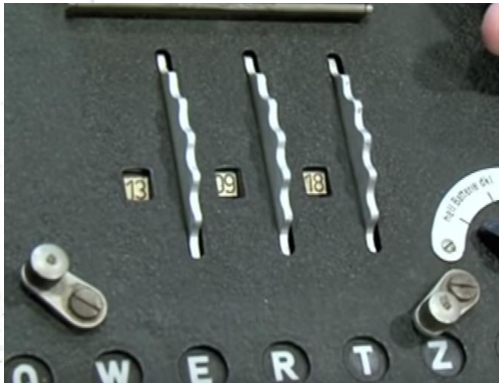
Geheim!

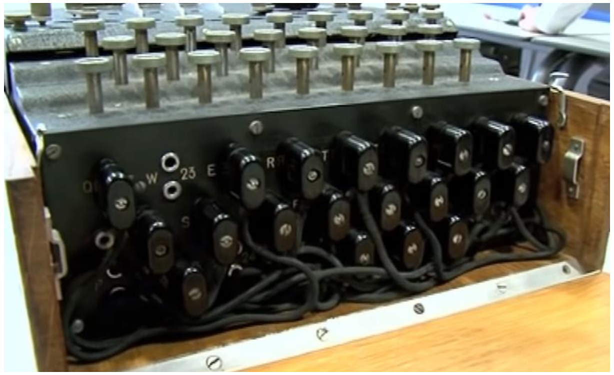
Nicht ins Flugzeug mitnehmen!

Sonder-Maschinenschlüssel BGS

08 ❊

Datum	Walzenlage			Ringstellung			Steckerverbindungen										Kenngruppen			
31.	I	II	V	10	14	02	BF	SD	AY	HG	OU	QC	WI	RL	XP	ZK	yqv	vuc	xxo	gvf
30.	V	IV	I	04	25	01	DI	ZL	RX	UH	QK	PC	VY	GA	SO	EM	mqy	vts	gvt	csx
29.	III	V	II	13	11	06	ZM	BQ	TP	YX	FK	AR	WH	SO	NJ	DG	aky	vdv	oyo	tzt
28.	I	III	II	09	16	12	NE	MT	RL	OY	HV	IU	GK	FW	PZ	XC	nfh	vco	tur	wnb
27.	III	II	I	06	03	15	BF	GR	SZ	OM	WQ	TY	HE	JU	XN	KD	bec	jmv	vtp	xdb
26.	I	III	V	19	26	08	GS	VD	CQ	LE	HI	BO	JP	UZ	FT	RN	wvu	yem	buz	rjk
25.	II	I	IV	05	01	16	KA	ZH	QP	GR	MF	LJ	OT	EN	BD	YW	ktv	muq	cqm	cpm
24.	III	II	IV	22	02	06	PI	KM	JB	YU	QS	OV	ZA	GW	CH	XF	zcd	iwo	urp	glg
23.	IV	III	II	08	11	07	SX	TD	QP	HU	FB	YN	CO	IK	WE	GZ	epm	mgz	vqg	vsm
22.	I	V	II	13	02	26	GP	XH	IW	BO	NU	MD	SA	ZK	QR	LT	aam	mvy	jqq	wqm
21.	IV	I	V	17	24	03	XC	AQ	OT	UZ	HD	RG	KM	BL	NS	JW	ltl	blu	frk	xrh
20.	IV	I	III	15	22	12	PO	TV	QC	ZS	EX	WR	BJ	DK	FU	LA	non	lic	oxr	usr
19.	V	I	III	13	24	21	HA	GM	DI	VK	JP	YU	EF	TB	ZL	XQ	ecd	ciq	uvr	ppt
18.	IV	V	I	23	09	20	XF	PZ	SQ	GR	AJ	UO	CN	BV	TM	KI	fjh	sts	uqu	cft
17.	III	II	V	21	24	15	UT	ZC	YN	BE	PK	JX	RS	GF	IA	QH	oub	eci	pyf	rqi
16.	IV	III	V	07	01	13	IN	YJ	SD	UV	GF	BH	TK	QE	AR	OP	kex	paw	flw	onw
15.	I	IV	II	15	04	25	TM	IJ	VK	OY	NX	PR	WL	GA	BU	SF	sdr	pbu	byv	khb
14.	III	II	IV	10	23	21	WT	RE	PC	FY	JA	VD	OI	HK	NX	ZS	mhz	lff	lnq	giy
13.	V	I	II	14	04	12	AN	IV	LH	YP	WM	TR	XU	FO	ZB	ED	rqh	ucm	ldi	ods
12.	II	V	I	07	19	02	HR	NC	IU	DM	TW	GV	FB	ZL	EQ	OX	asy	xza	uvc	fmr
11.	I	V	IV	13	15	11	NX	EO	RV	GP	SU	DK	IT	FY	BL	AZ	gyd	iuq	ocb	vef
10.	V	II	I	09	20	19	FN	TA	YJ	SO	EG	PC	VD	KI	XH	WZ	pyz	ace	pru	uyc
9.	I	IV	V	14	10	25	VK	DW	LH	RF	JS	CX	PT	YB	ZG	MU	nyh	fbd	ohs	jrp
8.	IV	V	I	22	04	16	PV	XS	ZU	EQ	BW	CH	AO	RL	JN	TD	tck	rts	nro	mkl
7.	V	I	IV	18	11	25	TS	IK	AV	QP	HW	FM	DX	NG	CY	UE	mhw	lwb	mdm	ybe
6.	IV	I	III	02	17	20	KZ	FI	WY	MP	DS	HR	CU	XE	QV	NT	uwu	vdk	lrh	mgd
5.	I	V	IV	26	09	14	VW	LT	PB	FO	ZK	GS	RI	QJ	HM	XE	suw	tsv	nfp	yjc
4.	IV	III	V	07	01	12	QS	YA	XW	KR	MP	HT	DU	OV	CL	FZ	uby	usi	mhh	mwb
3.	I	II	V	05	16	03	FW	DL	NX	BV	KM	RZ	HY	IQ	EC	JU	tns	von	grw	axl
2.	III	I	II	12	22	17	DW	UO	PY	GR	FS	EQ	KT	CL	AI	ZB	smz	lbl	bkc	sym
1.	I	III	II	04	18	06	ZN	OM	CR	UI	KP	WQ	SE	JV	LX	TF	ghr	vqv	cya	ayl





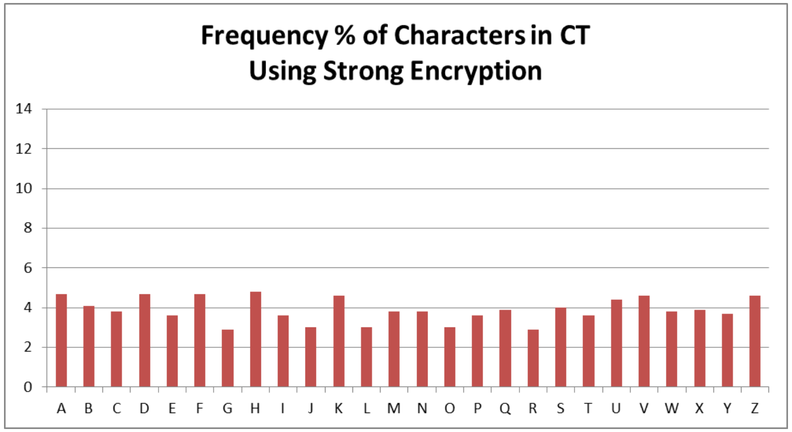
The Enigma Cipher

- The way in which the wheels rotate
- The fact it performs three substitutions with the wheel and once with the plug board.

Why Enigma is hard

- The characters in PT aren’t converted to a single output character in the CT, meaning a much more distributed frequency of characters, e.g. the PT “AAA” could be a CT of “TXO”
  - Much less correlation between PT and CT and any pattern observed in CT could simply be there by complete chance.

- 158,962,555,217,826,360,000 ways to set the enigma machine for each char compared to 26 using the Caesar cipher
  - Impossible to decrypt a CT using a purely ***brute force search***



Vulnerabilities in the enigma system

- The key has to be physically transported and stored in paper form, if the key book is captured the other side can decode messages for a month.

- If messages are sent regularly with repetitive information found in the same places within the messages with the same key used some of the key settings can eventually be deduced analytically.
  - German weather reports were always formatted in exactly the same way and dispatched many times a day using the same key, allowing the allies to eventually break Enigma.

- Crucially: It seems like there are no patterns in enigma but there still are!

- Wheels are re used, wheel positions are re used, plug board configurations are re used each day.

Exercise 2:

- Given what you’ve seen in the Caesar cipher and enigma system I want you to discuss:

1. Is there such thing as a perfectly secure cipher and key ?

2. If so what would be the qualities of this key and cipher be that the Caesar cipher and enigma machine don’t have?

Hint:

Think about why the enigma machine is more secure than the Caesar cipher and then imagine if you carried on making it more secure what the most extreme encryption machine would be?

The One Time Pad: A Perfect Key!

- The perfect key is one which is **completely random** and only ever used for a single message, the length of the key is the same as the length of the PT, this is called the “One Time Pad”

- If the key is the same length as the message then there is no **meaningful repetition** across the message which can reveal anything about the key. The mapping of each character in PT to CT has no relevance to the mapping of any other character. **There are no patterns!**

- If it is only ever used for one message then even if that message is intercepted analysis of the message has no relevance on the encryption of any other messages.

- It is mathematically impossible to break a one time pad system, It’s the definition of perfect encryption!

- Has been used for very high level Military communications and direct communication between states such as the US and USSR during the height of the cold war.
  - The Washington Moscow hotline.

LOW SPEED CRYPTOGRAPHIC EQUIPMENT
HOT LINE
East German T63-SU12 Teleprinter
This Machine was used as part of the Washington to Moscow Hotline CA. 1963-1980

Couldn’t you brute force it?

- The number of strings which can exist in a one time pad for the regular alphabet in lower case is 26^n where *n* is the message length.
- A CT of length 8 then has 26^8 = 208,827,064,576 possible PT strings, an exponential increase relative to the length of the message.
- This includes not just gibberish string such as “aoisjdeq” or “mfgmrpaq” which we can rule out but also every possible string which can ever exist of length 8 including every other legitimate 8 letter word e.g. “champion”, “abstract”, “aircraft”, “describe”, “friendly”
- It’s therefore impossible to tell what the 8 letter word the PT was because when doing a brute force search you would also uncover all of these other possible legitimate words which could have been sent, how are you supposed to know which specific word the key actually reveals?
- Additional Video Explanation: https://youtu.be/FlIG3TvQCBQ

Key length

- In general then the longer a key is then the more secure a message which is encrypted using it also is.

- A shorter key results in more **meaningful repetition** within the message
  - This is because each part of the key needs to be used multiple times to encrypt different parts of the message.

- This means that patterns start to reoccur across the message the longer the message is.

- A key which is as long as the message itself results in no **meaningful repetition** within the message.

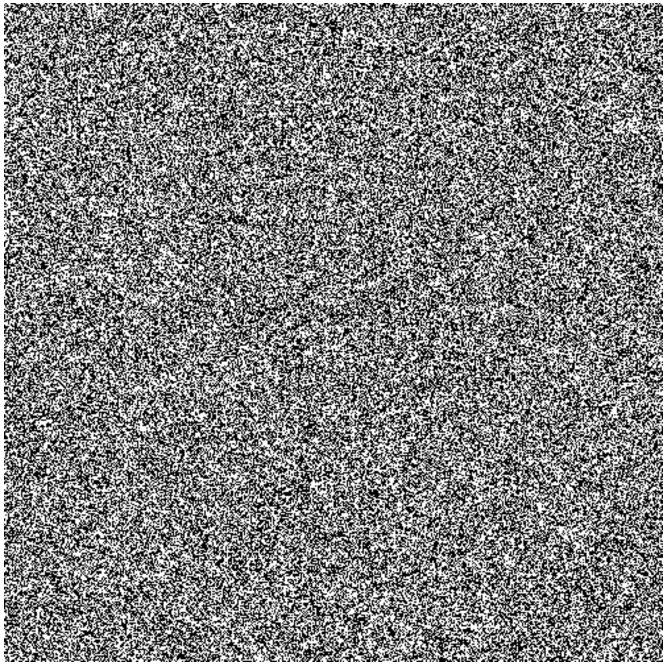
Why don’t we use the one time pad for everything?

- Although a key of equal length to the message is perfectly secure it’s also extremely impractical.
- Say you want to send 50GB of encrypted data.
  - To use a one time pad you would also have to generate a 50GB random key, share that key with the other party and then use it to encrypt and decrypt the 50GB of data.
  - This is going to be computationally very slow to perform and if you’re on a low power device it will use a lot of power!
  - A much shorter key can be used to perform much more efficient encryption and decryption whilst still being extremely secure.

What actually is Randomness?

- It’s good to understand some ideas about randomness in order to appreciate why people worry about randomness in cryptography.

- There are two ways to think about what randomness actually is.
  - **Nondeterminism**
  - **Determinism**



Non-determinism

- Some people believe there is randomness inherently present in the universe, in other words some events “just happen” without being determined by other events which lead up to them.
  - These People would say the universe is **Nondeterministic**,
  - A non determinist would say if you roll a dice there is 1/6 chance of it landing on any given side.

Determinism

- Others believe that every event that happens in the future is **completely determined** by the events which preceded it, this is known as **Determinism.**

- **Determinists** believe if science and our understanding of the universe were complete, I.e. we could compute the effect of every variable in the universe and knew it’s initial configuration there would be no perceived randomness to us.
  - With enough computing power we could determine every event in the future that will happen based on the current state of the universe and its previous states.

- To a **Determinist** Randomness is therefore a measure of our *inability to understand every variable at play within a given system*.

- A determinist would say the number rolled on a dice isn’t a case of a 1/6 chance but based on how it was rolled, it’s weight, shape, the environment it was rolled in etc.

Nondeterminism vs Determinism Example: The question of Freewill

- One of the biggest questions in philosophy is whether humans are Deterministic or Nondeterministic.

- The vast majority of people intuitively believe they are Nondeterministic, If you believe that you have free will as a human then you are a **Nondeterminist**.

  – If you have free will when you make a decision about something you ***consciously chose to make that decision*** and had the option to have chosen otherwise.

  – Alternatively if you are deterministic when you made the decision you behaved ***completely predictably.*** How you behaved was simply the result of your own genetics, prior life experiences and the circumstances in which the decision was made. E.g. did you have a split second or days to think about it.

  – Given a complete understanding of these variables we could say you were already ***guaranteed*** to have made the decision the way you made it. ***There was no possibility of you ever selecting another option.***

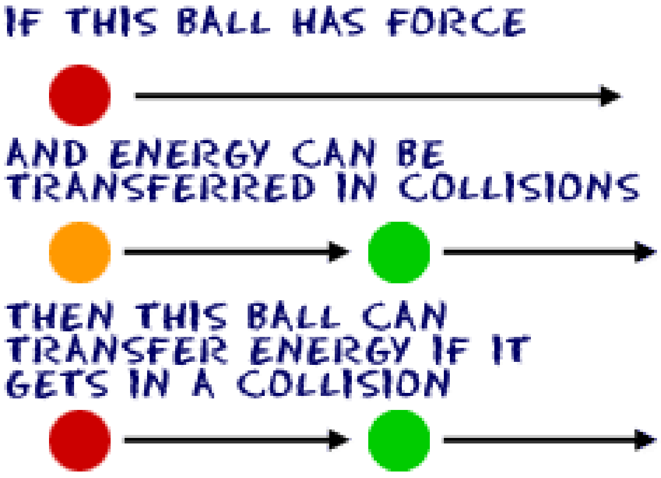
- This question has huge implications because without free will ultimately you can't be held to account for any action you take. If you commit a crime then you were already going to have committed the crime due to other factors.

Scientific Reasoning

- ***Science is the belief that the future will behave like the past.***

- Science is about trying to take something which appears **<u>Nondeterministic</u>** and show that it will behave **<u>Deterministically</u>** once we understand that behaviour.

- Some phenomena were deemed nondeterministic for thousands of years and are now considered more or less completely deterministic.


IF THIS BALL HAS FORCE
AND ENERGY CAN BE TRANSFERRED IN COLLISIONS
THEN THIS BALL CAN TRANSFER ENERGY IF IT GETS IN A COLLISION

Exercise 3: Deterministic Processes

- Can you think of anything which historically seemed completely Random and Nondeterministic and is now largely Deterministic and not Random?
- Take 10 minutes as a group to try and come up with a list of things.

Determinism Through Science Example: Weather Forecasting

- Hundreds of years ago the weather seemed largely Random, other than general trends in the different seasons, Spring, Summer, Autumn, Winter.

- Different cultures made sacrifices and prayed to the gods to deliver specific weather conditions which were desirable to them.

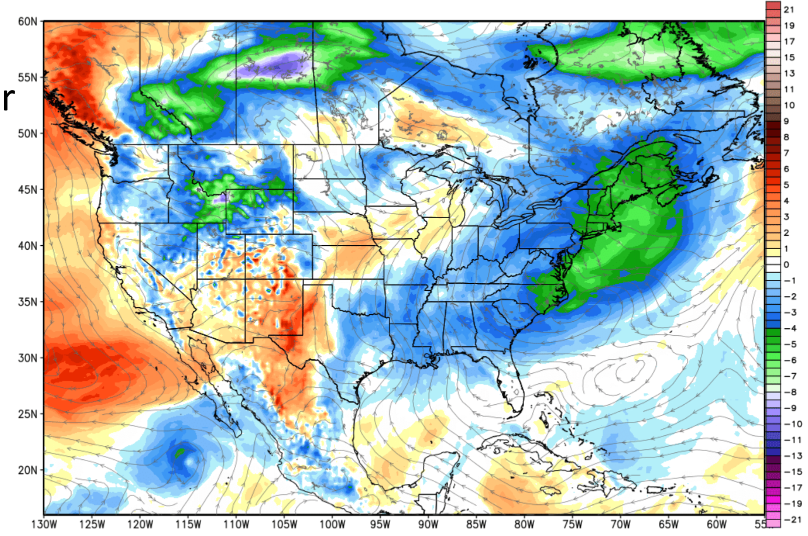
- Over time we gradually understood how weather systems worked and were able to use powerful computers and huge data sets to simulate their behaviour and improve our predictions.

- The result: we still can’t perfectly predict the weather but for the most part we can predict it to a very high degree of accuracy and we have a good idea of how the climate and weather will change over longer periods 5,10, 20 years…

- We took something which seemed completely random and made it very predictable.

ECMWF 850 hPa Temp Anomaly [°C] & Wind Streams
INIT: 12Z28JUN2017 fx: [012] hr --> Thu 00Z29JUN2017

Min|Max −10.6° | 7.4°C



Parallel | Test data for Cycle 43r3 Upgrade to HRES July 2017 | Data Copyright ECMWF | WeatherBELL

Randomness in Cryptography.

- In Cryptography we rely on having random values in order to generate secure keys which can’t be easily predicted.

- But how do you generate a truly “Random” key?

- Randomness is a relative concept as just illustrated.

- Randomness is also a scale, some things are more random than others.

- For practical purposes the more random something is the harder it is to consistently predict how it will behave using methods we have so far developed as humans.
  - We shouldn’t be able to use a methodical process to determine the key somebody is using.

- <u>The more Random a key the more secure it is.</u>

Generating a random key

- Some natural processes generate values which as humans we have no current way of predicting.
- Radiation is the most popular way of doing this
- https://www.youtube.com/watch?v=SxP30euw3-0

How does a computer generate a random value?

- The Problem: Computers fundamentally are completely deterministic.
- Computers follow algorithms, sets of specific instructions and manipulate the data they are given exactly based on their code.
- Therefore computers cannot generate perfectly random numbers because they have to follow a process to generate the random numbers one after another.
- Computers therefore generate ***pseudo random*** numbers.
- ***Pseudo random*** numbers are numbers which appear random but aren’t random in the way we consider some processes in nature to be random.
- In other words there is a process humans understand that has been used to generate them.
- Crucially if the computer is asked to generate more ***pseudo random*** numbers the numbers don’t follow a sequence which allows the observer of those numbers to generate the next number in the sequence.

Generating Pseudo Random values with a computer

- A computer generates a pseudo random number from what is known as a ***Seed***

- A seed is a number taken from a source outside the computer system, a value provided by the outside world.

- Most computers use some aspect of the current time as the seed (in itself not random).

- The seed then needs to be “grown” to make the number appear random

Middle Squares Method

- Take the time since some specified point

e.g. milliseconds past the latest minute: 2315

- Multiply the seed by itself 2315 * 2315 = 5,359,225

- Take the middle three digits of this number = 592

- Multiply 5,359,225 by itself again to get 28,721,292,600,625

- Take the middle three digits of this number (292) and concatenate with the previous three = 592292

Takeaways from the Lecture

- Cryptography Can be simple or extremely complex, it all comes down to the sophistication of the key and the cipher.

- Ultimate Goal: Make the Cypher text as hard for an interceptor to decrypt as possible while still allowing the other party to easily perform the decryption

- Stronger ciphers have greater a greater amount of randomness or stronger pseudo randomness in the design and selection of the key.

Further Activities for Today

- Read about the Enigma machine
- Think about how we solve the problem of transferring the key

Further Study

The Enigma machine video explanation:

https://www.youtube.com/watch?v=G2_Q9FoD-oQ