The Enigma machine	Season	03
	Episode	16
	Time frame	2 periods

Prerequisites : Main cryptographic techniques

Objectives :
- Discover the workings of the Enigma machine.
- Count the number of possibilities offered by the machine.

Materials :
- 6 *copies of each fact sheet.*
- $6 \times 3 \times 3 = 54$ *copies of the Enigma machine setup page.*
- $6 \times 4 = 24$ *copies of the rotors page.*

1 – Expert teams — 25 mins

The class is divided in 6 groups. Each group is given a fact sheet about one of the aspects of the Enigma machine. They have 25 minutes to understand the explanation and find a partial formula for the number of possibilities offered by their part of the machine.

2 – Mixing the teams — 30 mins

The class is once again divided in 6 groups, with one member from each of the 6 expert groups. They have 30 minutes to communicate and understand the global workings of the Enigma machine, and compute the total number of possibilities.

3 – Coding and decoding messages — 1 period

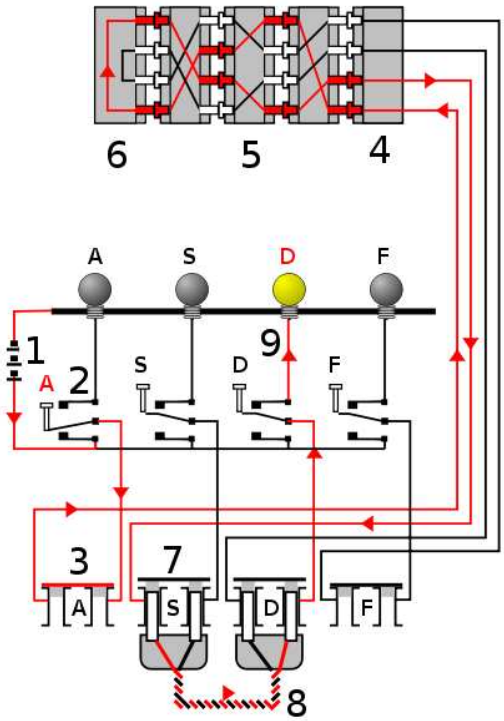
Each group has to code and decode some messages and gets mark depending on the number of correct codings and decodings.

The overall design of Enigma	Season	03
	Episode	16
	Document	Fact sheet 1

An Enigma machine is an electro-mechanical rotor machines that was used for the encryption and decryption of secret messages by the German army during World War II. Like other rotor machines, the Enigma machine is a combination of mechanical and electrical subsystems.

The mechanical subsystem consists of a keyboard ; a set of rotating disks called rotors arranged adjacently along a spindle ; and one of various stepping components to turn one or more of the rotors with each key press.

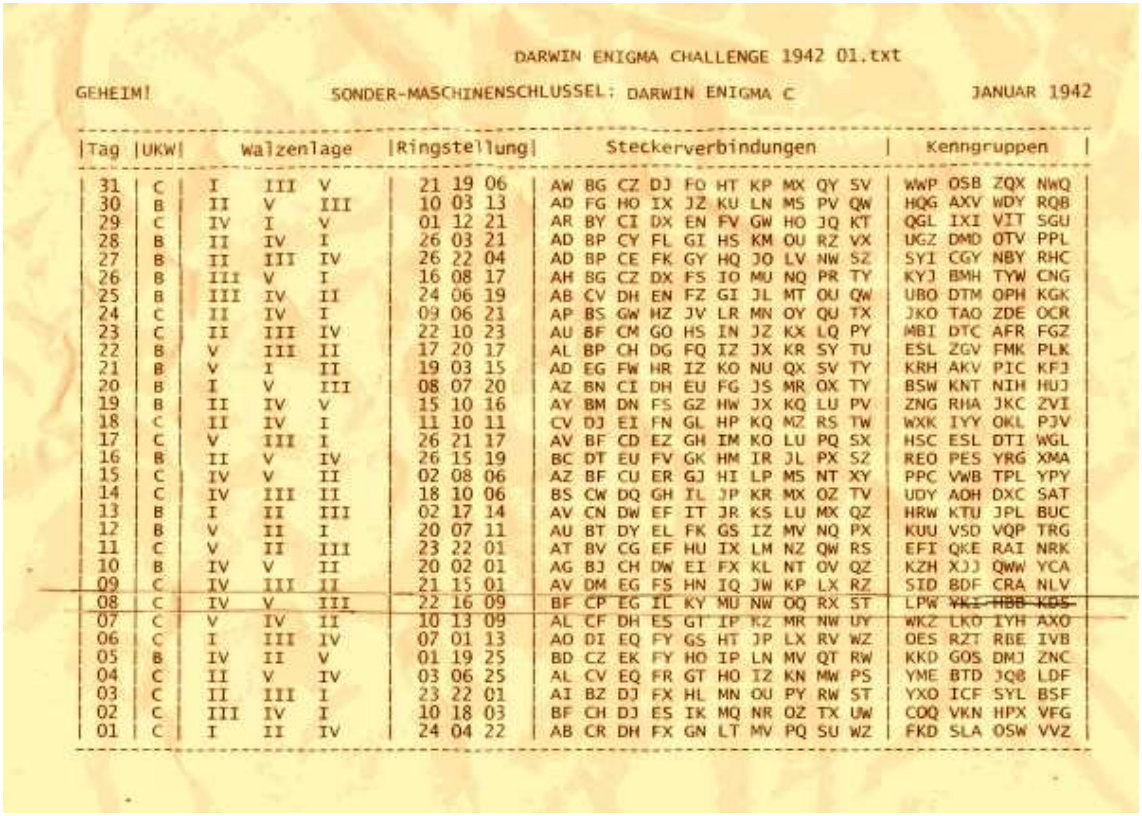
The mechanical parts act in such a way as to form a varying electrical circuit. When a letter key is pressed, the circuit is completed ; current flows through the various components in their current configuration and ultimately lights one of the display lamps, indicating the output letter. For example, when encrypting a message starting with the letters ANX. . . , the operator would first press the A key, and the Z lamp might light, so Z would be the first letter of the ciphertext. The operator would next press N, and then X in the same fashion, and so on.



To illustrate the detailed operation of Enigma, please refer to the wiring diagram on the left. To simplify the example, only four components of a complete Enigma machine are shown. In reality, there are 26 lamps and keys, several plugs (varied with model) and rotor wirings inside the rotors (at least three were installed).
Current flows from the battery **(1)** through a depressed bi-directional letter-switch on a keyboard **(2)** to the plugboard **(3)**. The current winds through the (unused in this instance, so shown closed) plug **(3)**, then via the entry wheel **(4)** through the wiring of the three installed rotors **(5)**, and enters the reflector **(6)**. The reflector returns the current, via an entirely different path, through the rotors **(5)** and entry wheel **(4)**, proceeding through plug 'S' connected with a cable **(8)** to plug 'D', and another bi-directional switch **(9)** to light the appropriate lamp.

In German military usage, communications were divided up into a number of different networks, all using different settings for their Enigma machines. Each unit operating on a network was assigned a settings list for its Enigma for a period of time. For a message to be correctly encrypted and decrypted, both sender and receiver had to set up their Enigma in the same way ; the rotor selection and order, the starting position and the plugboard connections must be identical. All these settings (together the key in modern terms) must have been established beforehand, and were distributed in codebooks.
An Enigma machine's initial state, the cryptographic key, has several aspects :

- Wheel order (Walzenlage) : the choice of rotors and the order in which they are fitted.
- Initial position of the rotors : chosen by the operator, different for each message.
- Ring settings (Ringstellung) : the position of the alphabet ring relative to the rotor wiring.
- Plug settings (Steckerverbindungen) : the connections of the plugs in the plugboard.



DARWIN ENIGMA CHALLENGE 1942 01.txt

GEHEIM! SONDER-MASCHINENSCHLUSSEL: DARWIN ENIGMA C JANUAR 1942

Tag	UKW	Walzenlage	Ringstellung	Steckerverbindungen	Kenngruppen
31	C	I III V	21 19 06	AW BG CZ DJ FO HT KP MX QY SV	WWP OSB ZQX NWQ
30	B	II V III	10 03 13	AD FG HO IX JZ KU LN MS PV QW	HQG AXV WDY RQB
29	C	IV I V	01 12 21	AR BY CI DX EN FV GW HO JQ KT	QGL IXI VIT SGU
28	B	II IV I	26 03 21	AD BP CY FL GI HS KM OU RZ VX	UGZ DMD OTV PPL
27	B	II III IV	26 22 04	AD BP CE FK GY HQ JO LV NW SZ	SYI CGY NBY RHC
26	B	III V I	16 08 17	AH BG CZ DX FS IO MU NQ PR TY	KYJ BMH TYW CNG
25	B	III IV II	24 06 19	AB CV DH EN FZ GI JL MT OU QW	UBO DTM OPH KGK
24	C	II IV I	09 06 21	AP BS GW HZ JV LR MN OY QU TX	JKO TAO ZDE OCR
23	C	II III IV	22 10 23	AU BF CM GO HS IN JZ KX LQ PY	MBI DTC AFR FGZ
22	B	V III II	17 20 17	AL BP CH DG FQ IZ JX KR SY TU	ESL ZGV FMK PLK
21	B	V I II	19 03 15	AD EG FW HR IZ KO NU QX SV TY	KRH AKV PIC KFJ
20	B	I V III	08 07 20	AZ BN CI DH EU FG JS MR OX TY	BSW KNT NIH HUJ
19	B	II IV V	15 10 16	AY BM DN FS GZ HW JX KQ LU PV	ZNG RHA JKC ZVI
18	C	II IV I	11 10 11	CV DJ EI FN GL HP KQ MZ RS TW	WXK IYY OKL PJV
17	C	V III I	26 21 17	AV BF CD EZ GH IM KO LU PQ SX	HSC ESL DTI WGL
16	B	II V IV	26 15 19	BC DT EU FV GK HM IR JL PX SZ	REO PES YRG XMA
15	C	IV V II	02 08 06	AZ BF CU ER GJ HI LP MS NT XY	PPC VWB TPL YPY
14	C	IV III II	18 10 06	BS CW DQ GH IL JP KR MX OZ TV	UDY AOH DXC SAT
13	B	I II III	02 17 14	AV CN DW EF IT JR KS LU MX QZ	HRW KTU JPL BUC
12	B	V II I	20 07 11	AU BT DY EL FK GS IZ MV NQ PX	KUU VSD VQP TRG
11	C	V II III	23 22 01	AT BV CG EF HU IX LM NZ QW RS	EFI QKE RAI NRK
10	B	IV V II	20 02 01	AG BJ CH DW EI FX KL NT OV QZ	KZH XJJ QWW YCA
09	C	IV III II	21 15 01	AV DM EG FS HN IQ JW KP LX RZ	SID BDF CRA NLV
08	C	IV V III	22 16 09	BF CP EG IL KY MU NW OQ RX ST	LPW YKI HBB KDS
07	C	V IV II	10 13 09	AL CF DH ES GT IP KZ MR NW UY	WKZ LKO IYH AXO
06	C	I III IV	07 01 13	AO DI EQ FY GS HT JP LX RV WZ	OES RZT RBE IVB
05	B	IV II V	01 19 25	BD CZ EK FY HO IP LN MV QT RW	KKD GOS DMJ ZNC
04	C	II V IV	03 06 25	AL CV EQ FR GT HO IZ KN MW PS	YME BTD JQB LDF
03	C	II III I	23 22 01	AI BZ DJ FX HL MN OU PY RW ST	YXO ICF SYL BSF
02	C	III IV I	10 18 03	BF CH DJ ES IK MQ NR OZ TX UW	COQ VKN HPX VFG
01	C	I II IV	24 04 22	AB CR DH FX GN LT MV PQ SU WZ	FKD SLA OSW VVZ

In fact, the Enigma cipher machine consists of five variable features :

1. a plugboard which can contain from zero to thirteen dual-wired cables ;
2. three ordered (left to right) rotors which wire twenty-six input contact points to twenty-six output contact points positioned on alternate faces of a disk ;
3. twenty-six serrations around the periphery of the rotors which allow the operator to specify an initial rotational position for the rotors ;
4. a moveable ring on each of the rotors which controls the rotational behavior of the rotor immediately to the left by means of a notch ;
5. a reflector half-rotor (which do not in fact rotate) to fold inputs and outputs back onto the same face of contact points.

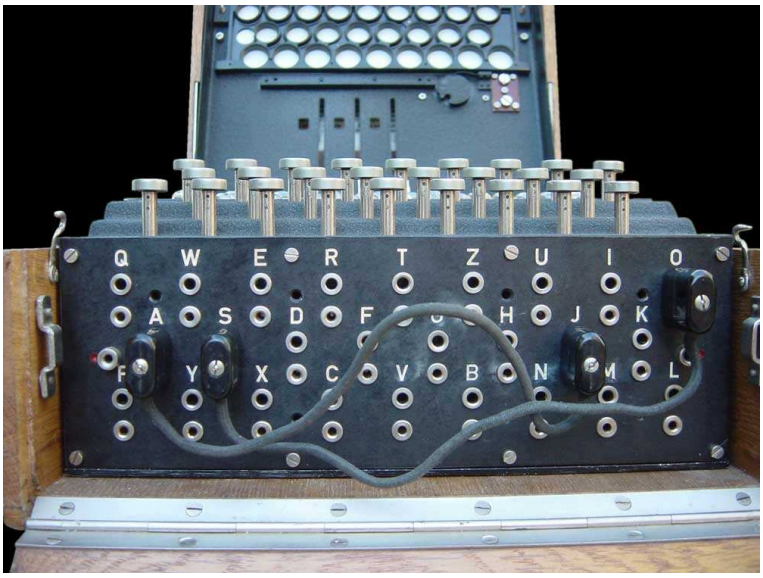
Your task : Understand the overall workings of the Enigma machine and be ready to put together the pieces of information brought by other students. You will be the team leader.

The plugboard	Season	03
	Episode	16
	Document	Fact sheet 2

An Enigma machine is an electro-mechanical rotor machines that was used for the encryption and decryption of secret messages by the German army during World War II. Like other rotor machines, the Enigma machine is a combination of mechanical and electrical subsystems.

The first variable component was the plugboard. Twenty-six (A to Z) dual-holed sockets were on the front panel of the machine. A dual-wired plugboard cable could be inserted making a connection between any pair of letters. Enigma cryptographers had a choice of how many different cables could be inserted (from zero to thirteen) and which letters were connected.

A cable placed onto the plugboard connected letters up in pairs ; for example, E and Q might be a connected pair. The effect was to swap those letters before and after the main rotor scrambling unit. For example, when an operator presses E, the signal was diverted to Q before entering the rotors. Several such steckered pairs, up to 13, might be used at one time. However, normally only 10 pairs were used at any one time.
The plugboard contributed a great deal to the strength of the machine's encryption : more than an extra rotor would have done. Enigma without a plugboard (known as unsteckered Enigma) can be solved relatively straightforwardly using hand methods ; these techniques are generally defeated by the addition of a plugboard, and Allied cryptanalysts resorted to special machines to solve it.



Your task : Understand the workings of the plugboard and find out the number of different settings there were, depending on the number p of plugs used. You will be the plugboard specialist in your team.

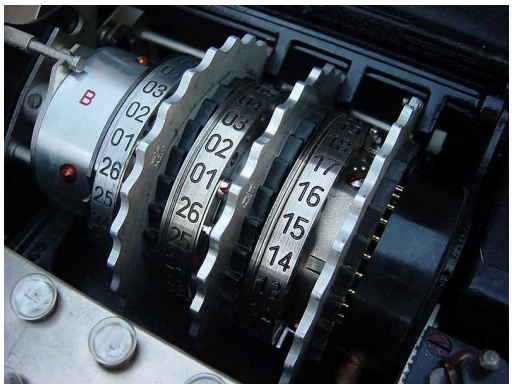
Rotors inner circuitry	Season	03
	Episode	16
	Document	Fact sheet 3

An Enigma machine is an electro-mechanical rotor machines that was used for the encryption and decryption of secret messages by the German army during World War II. Like other rotor machines, the Enigma machine is a combination of mechanical and electrical subsystems.

The second variable component was the three ordered (left to right) rotors which connected twenty-six input contact points to twenty-six output contact points positioned on alternate faces of a disc.

The rotors (alternatively wheels or drums, Walzen in German) formed the heart of an Enigma machine. Each rotor was a disc approximately 10 cm (3.9 in) in diameter with brass spring-loaded pins on one face arranged in a circle ; on the other side are a corresponding number of circular electrical contacts. The pins and contacts represent the alphabet – typically the 26 letters A to Z. When the rotors were mounted side-by-side on the spindle, the pins of one rotor rest against the contacts of the neighbouring rotor, forming an electrical connection. Inside the body of the rotor, 26 wires connected each pin on one side to a contact on the other in a complex pattern. Most of the rotors were identified by Roman numerals and each issued copy of rotor I was wired identically to all other rotors I.

By itself, a rotor will perform only a very simple type of encryption – a simple substitution cipher. For example, the pin corresponding to the letter E might be wired to the contact for letter T on the opposite face, and so on. The Enigma's complexity, and cryptographic security, came from using several rotors in series (usually three) and the regular stepping movement of the rotors, thus implementing a poly-alphabetic substitution cipher.



Your task : Understand the inner workings of the rotors and find out the number of different settings there were for each disk, and for three consecutive disks. You will be the inner rotors specialist in your team.

Rotors positioning	Season	03
	Episode	16
	Document	Fact sheet 4

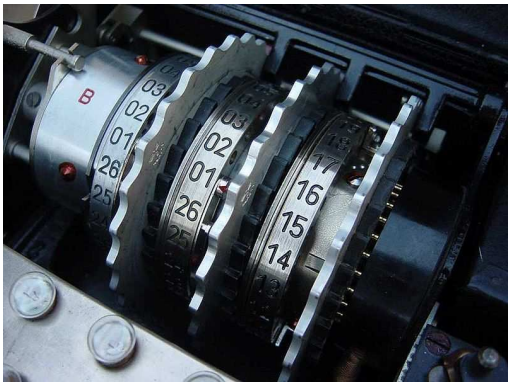
An Enigma machine is an electro-mechanical rotor machines that was used for the encryption and decryption of secret messages by the German army during World War II. Like other rotor machines, the Enigma machine is a combination of mechanical and electrical subsystems.

The third variable component of Enigma was the initial rotational position of the three rotors containing the wired discs. This was specified by the cryptographers and set by the machine operators by means of twenty-six serrations around the rotor periphery.

The rotors (alternatively wheels or drums, Walzen in German) formed the heart of an Enigma machine. By itself, a rotor will perform only a very simple type of encryption – a simple substitution cipher. For example, the pin corresponding to the letter E might be wired to the contact for letter T on the opposite face, and so on. The Enigma's complexity, and cryptographic security, came from using several rotors in series (usually three or four) and the regular stepping movement of the rotors, thus implementing a poly-alphabetic substitution cipher.

When placed in an Enigma, each rotor can be set to one of 26 possible positions. When inserted, it can be turned by hand using the grooved finger-wheel which protrudes from the internal Enigma cover when closed. So that the operator can know the rotor's position, each had an alphabet tyre (or letter ring) attached to the outside of the rotor disk, with 26 characters (typically letters) ; one of these could be seen through the window, thus indicating the rotational position of the rotor.

The Army and Air Force Enigmas were used with several rotors. From December 1938, there were five, from which three were chosen for insertion in the machine for a particular operating session. Rotors were marked with Roman numerals to distinguish them : I, II, III, IV and V.

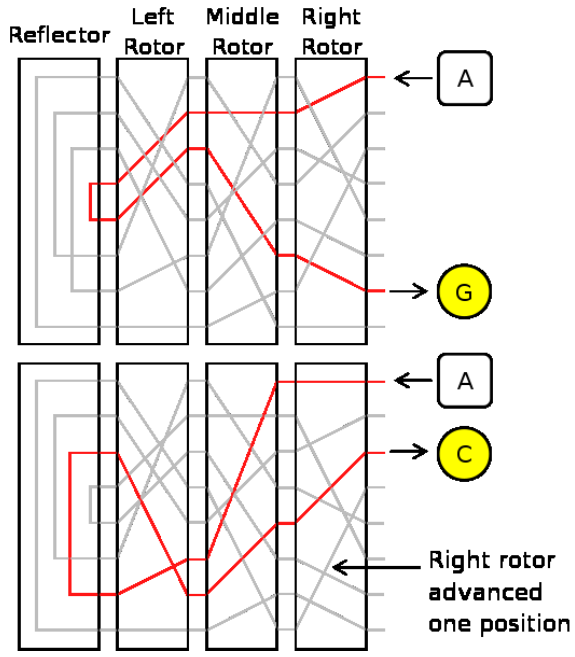


Your task : Understand rotors positioning and find out the number of different settings there were for each disk, and for three consecutive disks chosen among five possible disks. You will be the rotors positioning specialist in your team.

Stepping motion	Season	03
	Episode	16
	Document	Fact sheet 5

An Enigma machine is an electro-mechanical rotor machines that was used for the encryption and decryption of secret messages by the German army during World War II. Like other rotor machines, the Enigma machine is a combination of mechanical and electrical subsystems.

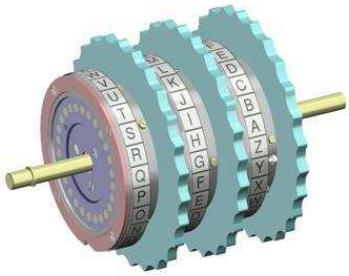
The fourth variable component of the machine was a moveable ring on each of the rotors ; each ring contained a notch in a specific location. The purpose of the notch was to force a rotation of the rotor immediately to the left when the notch was in a particular position



The rotors (alternatively wheels or drums, Walzen in German) formed the heart of an Enigma machine. By itself, a rotor will perform only a very simple type of encryption – a simple substitution cipher. For example, the pin corresponding to the letter E might be wired to the contact for letter T on the opposite face, and so on.

To avoid merely implementing a simple (and easily breakable) substitution cipher, every key press caused one or more rotors to step before the electrical connections were made, and so changed the substitution alphabet used for encryption. This ensured that the cryptographic substitution would be different at each new rotor position, producing a more formidable polyalphabetic substitution cipher.

The rightmost rotor rotated every time a key was pressed. The rightmost rotor's notch forced a rotation of the middle rotor once every twenty-six keystrokes. The middle rotor's notch forced a rotation of the leftmost rotor once every 26 X 26 keystrokes. Since there were no more rotors, the leftmost rotor's notch had absolutely no effect whatsoever.



Your task : Understand the rotors stepping motion and find out the number of different settings there were for the position of the notches for three consecutive disks. You will be the stepping motion specialist in your team.

The reflector	Season	03
	Episode	16
	Document	Fact sheet 6

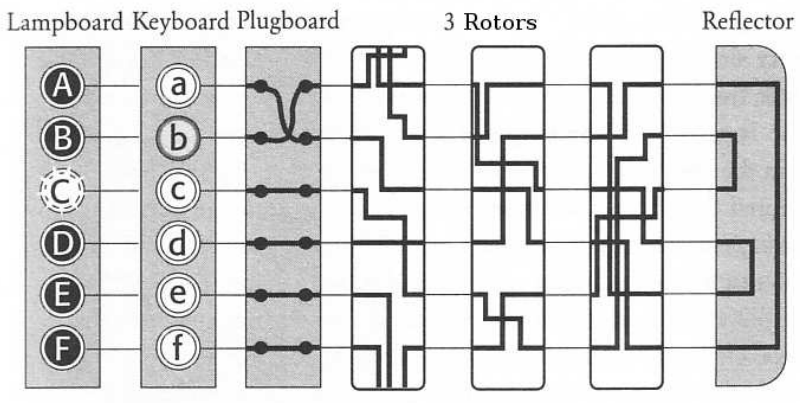
An Enigma machine is an electro-mechanical rotor machines that was used for the encryption and decryption of secret messages by the German army during World War II. Like other rotor machines, the Enigma machine is a combination of mechanical and electrical subsystems.

The fifth and final variable component of Enigma was the reflector. The reflector had twenty-six contact points like a rotor, but only on one face.

The reflector connected outputs of the last rotor in pairs, redirecting current back through the rotors by a different route. The reflector ensured that Enigma is self-reciprocal : conveniently, encryption was the same as decryption. However, the reflector also gave Enigma the property that no letter ever encrypted to itself. This was a severe conceptual flaw and a cryptological mistake subsequently exploited by codebreakers.

Thirteen wires internally connected the twenty-six contact points together in a series of pairs so that a connection coming in to the reflector from the rotors was sent back through the rotors a second time by a different route. The internal wiring could be constructed in the following fashion. When one end of the first wire was connected to contact point #1, the other side of the wire had twenty-five different contact points to which it could be connected.

Thus the first wire consumed two contact points and had twenty-five different possibilities. The second wire also consumed two contact points, and had only twenty-three different connection possibilities remaining from the unconsumed contact points. The third wire consumed two more contact points and had twenty-one possibilities for connection.



Your task : Understand the role and workings of the reflector and find out the number of different settings there were. You will be the reflector specialist in your team.

Coding and decoding with Enigma	Season	03
	Episode	16
	Document	Exercises

For each of the following exercises, you will have to set up a paper Enigma machine with :
- a choice of up to 10 plugs, each one witching two letters ;
- three rotors from the five available – for practical purposes you will first have to cut them out and tape two copies of each rotor side by side ;
- the initial position for each rotor ;
- the position of the notch for the first two rotors, that is the position which, we reached, will make the next rotor move.

For the first two exercises, the setup will be given and you will have to decode a message. For the last two, you will have to agree on a setup with another group, code a message, send it to the other group and decode their message. Each exercise is worth 5 points.
We will agree that the first rotor starts moving to the left after the first letter is coded (or decoded), and that we start back from the initial position at the beginning of a each new message. Also remember that the coding and decoding processes are exactly the same.

Exercise 1 – A simple message with a simple setup

- Use no cables.
- Pick disks I, II III, in that order.
- Set the starting positions as 1, 1, 1.
- Set the notches positions at 26, 26, 26.
- Decode the message NZAZL HICGI NF.

Exercise 2 – A simple message with a more complicated setup

- Look up the configuration for the day 31 on the overall design sheet.
- Set up the Enigma machine accordingly.
- Decode the message JMFLR PBDBT ZDJH

Exercise 3 – Coding and decoding a short message

- Agree on a complete setup with another group, then code a short message, with less than 20 characters.
- Send the ciphered message to the other group through the teacher.
- Decipher the message received from the other group.

Exercise 4 – Coding and decoding a longer message

- Agree on a complete setup with another group, then code a message with at least 60 characters.
- Send the ciphered message to the other group through the teacher.
- Decipher the message received from the other group.

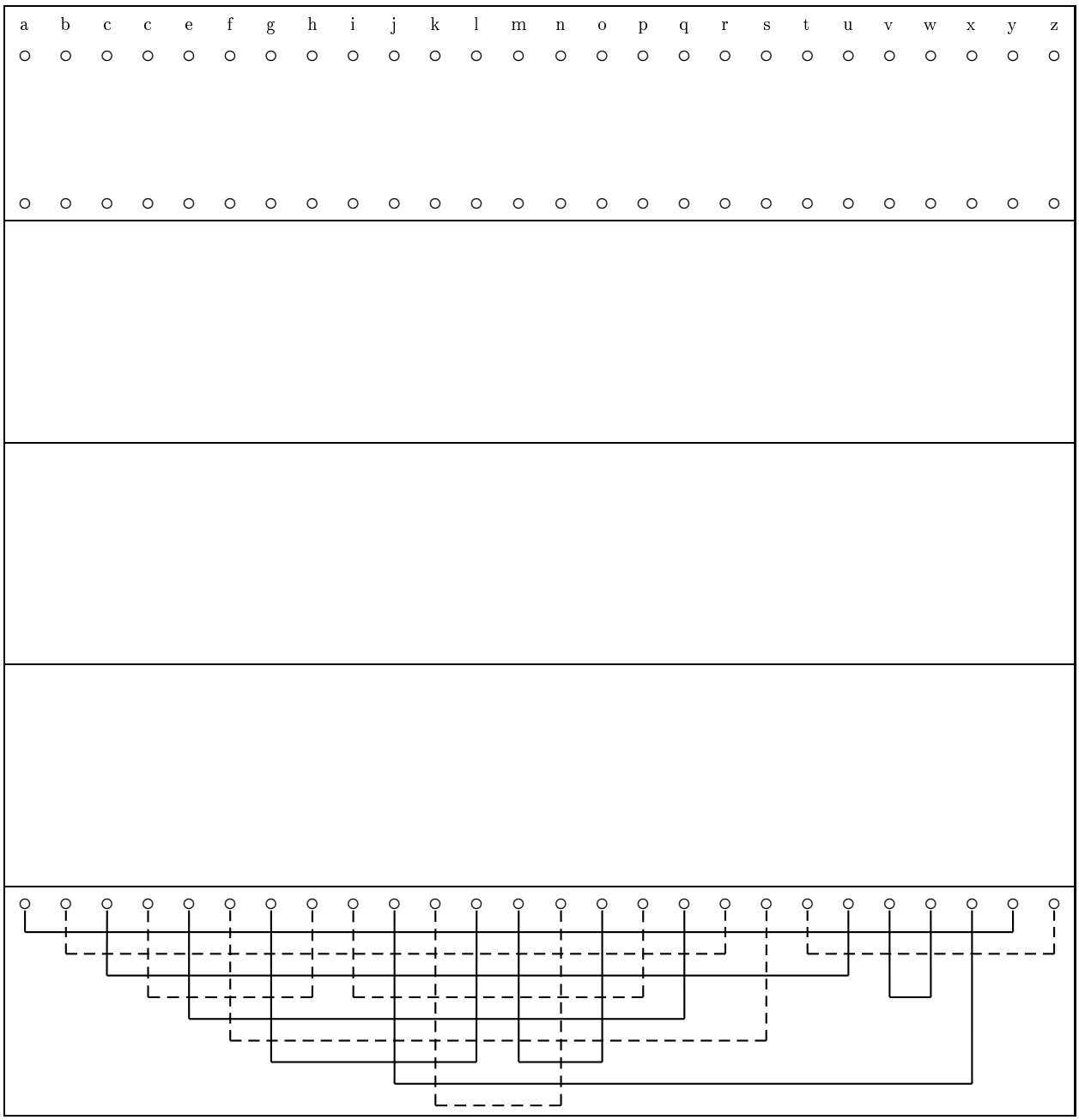
Coding and decoding with Enigma	Season	03
	Episode	16
	Document	Setup

Disks used : I – II – III – IV – V

Starting position and notch for disk 1 : ____ and ____

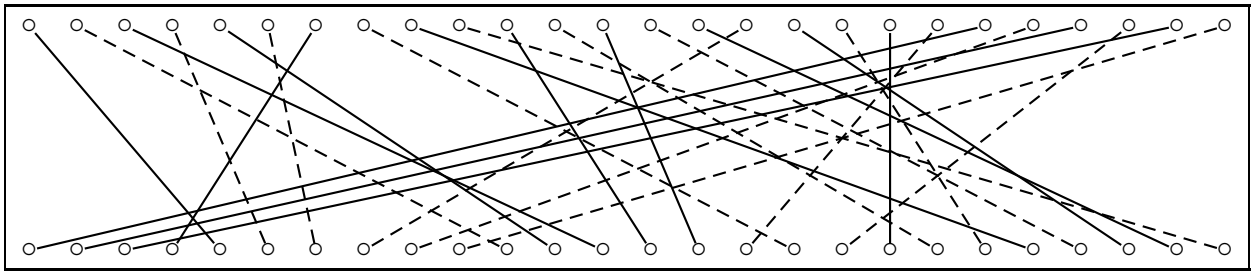
Starting position and notch for disk 2 : ____ and ____

Starting position and notch for disk 3 : ____ and ____

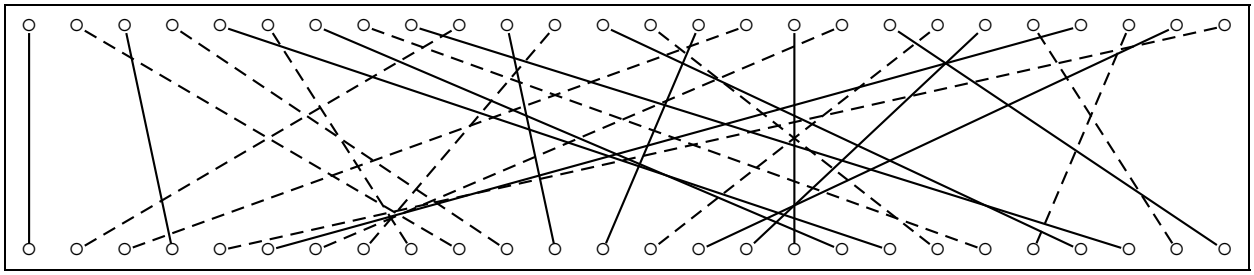


Document 1 Rotors

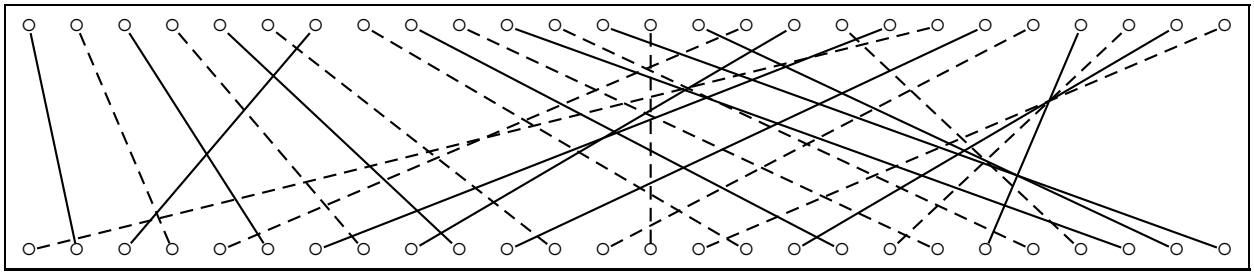
Rotor I



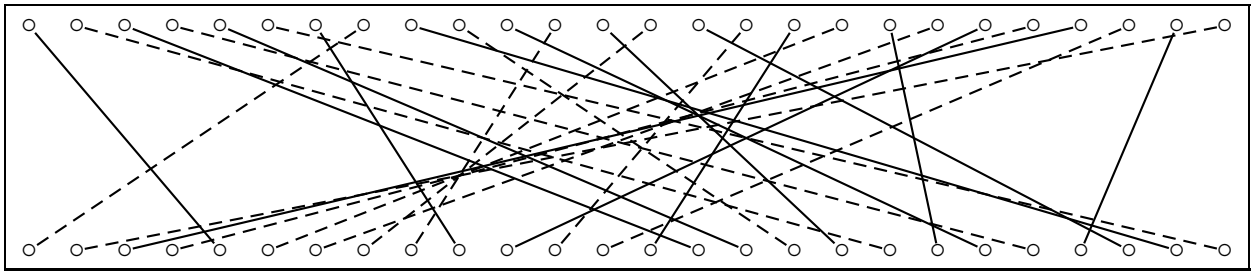
Rotor II



Rotor III



Rotor IV



Rotor V