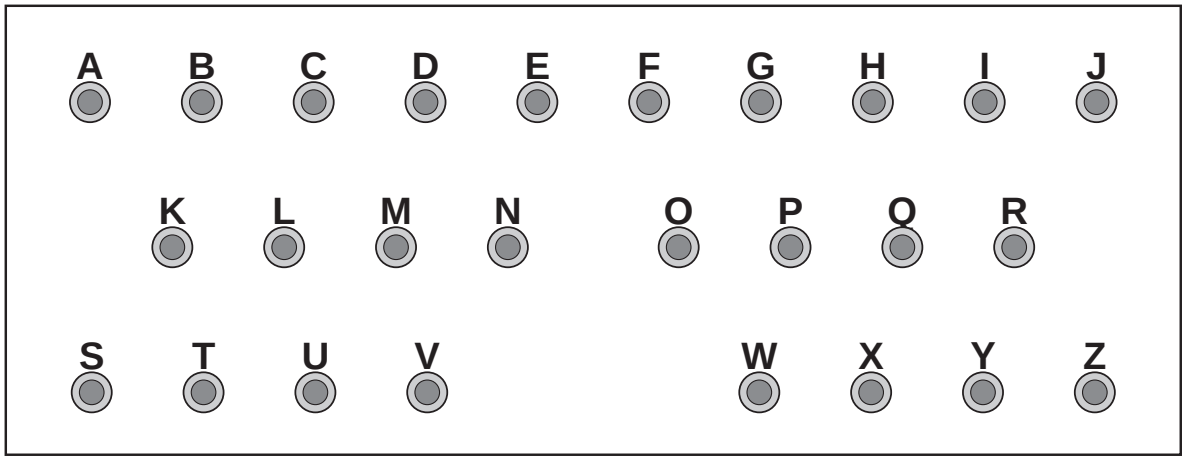
UNIT 20 *Enigma Cipher* Overhead Slides

Overhead Slides

OS 20.1 *Plugboard*



OS 20.2 *Formula for Choosing m Pairs for n Objects*

Number of ways of choosing m pairs for n objects

$$= \frac{n!}{(n-2m)!\,m!\,2^m}$$

(n is a whole number)

Example

Evaluate the formula when $n = 6$ and $m = 2$.

$$\text{Number of ways} = \frac{6!}{(6-4)!\,2!\,2^2}$$

$$= \frac{\qquad\qquad\qquad\qquad\qquad\qquad}{}$$

$$=$$

OS 20.3 *Number of Settings for Enigma Machine*

Number of settings = (no. of ways of positioning 5 rotors in 3 positions)

× (no. of different starting positions of rotor)

× (no. of ways of connecting plugboard)

= ☐ × ☐ × ☐

= ☐

OS 20.4 *'Paper Enigma'*

A Paper Enigma Machine

Shows the ciphers obtained for rotor positions "HAA" to "HAR" using a particular set of adjustments of the machine
(After enciphering each letter from your message, move down to the next rotor settings)

Rotor settings				Enigma Ciphers																								
				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**
1	**H**	**A**	**A**	W	O	F	S	Y	C	L	X	R	Q	P	G	T	V	B	K	J	I	D	M	Z	N	A	H	E	U
2	**H**	**A**	**B**	O	N	S	Y	T	P	Z	Q	M	K	J	X	I	B	A	F	H	V	C	E	W	R	U	L	D	G
3	**H**	**A**	**C**	Q	E	I	F	B	D	M	U	C	R	W	X	G	Y	S	V	A	J	O	Z	H	P	K	L	N	T
4	**H**	**A**	**D**	P	H	V	M	L	N	Y	B	U	Z	X	E	D	F	W	A	S	T	Q	R	I	C	O	K	G	J
5	**H**	**A**	**E**	S	T	F	H	R	C	O	D	X	U	L	K	W	V	G	Z	Y	E	A	B	J	N	M	I	Q	P
6	**H**	**A**	**F**	R	U	H	X	N	J	O	C	T	F	Q	W	Y	E	G	S	K	A	P	I	B	Z	L	D	M	V
7	**H**	**A**	**G**	Q	C	B	Z	O	R	M	P	V	X	T	W	G	S	E	H	A	F	N	K	Y	I	L	J	U	D
8	**H**	**A**	**H**	T	M	K	W	X	N	U	V	P	S	C	R	B	F	Z	I	Y	L	J	A	G	H	D	E	Q	O
9	**H**	**A**	**I**	Y	C	B	E	D	T	S	Q	M	L	U	J	I	Z	X	R	H	P	G	F	K	W	V	O	A	N
10	**H**	**A**	**J**	S	O	P	M	W	R	I	T	G	U	Q	Y	D	X	B	C	K	F	A	H	J	Z	E	N	L	V
11	**H**	**A**	**K**	X	D	P	B	F	E	S	V	R	T	Z	W	Q	U	Y	C	M	I	G	J	N	H	L	A	O	K
12	**H**	**A**	**L**	I	T	Z	S	Y	V	J	Q	A	G	W	N	P	L	U	M	H	X	D	B	O	F	K	R	E	C
13	**H**	**A**	**M**	G	K	R	W	T	O	A	Q	V	P	B	Z	X	Y	F	J	H	C	U	E	S	I	D	M	N	L
14	**H**	**A**	**N**	E	U	R	L	A	Y	P	W	M	O	S	D	I	T	J	G	X	C	K	N	B	Z	H	Q	F	V
15	**H**	**A**	**O**	S	V	H	F	X	D	O	C	R	P	M	U	K	Q	G	J	N	I	A	Z	L	B	Y	E	W	T
16	**H**	**A**	**P**	T	P	V	U	Q	L	N	R	O	W	Z	F	S	G	I	B	E	H	M	A	D	C	J	Y	X	K
17	**H**	**A**	**Q**	T	I	R	P	Y	Q	V	O	B	L	U	J	X	Z	H	D	F	C	W	A	K	G	S	M	E	N
18	**H**	**A**	**R**	Z	J	R	M	Q	U	P	N	O	B	Y	S	D	H	I	G	E	C	L	V	F	T	X	W	K	A

(The machine would go on making up more ciphers, but there is no more room here!)