

UNIT 20 *Enigma Cipher*

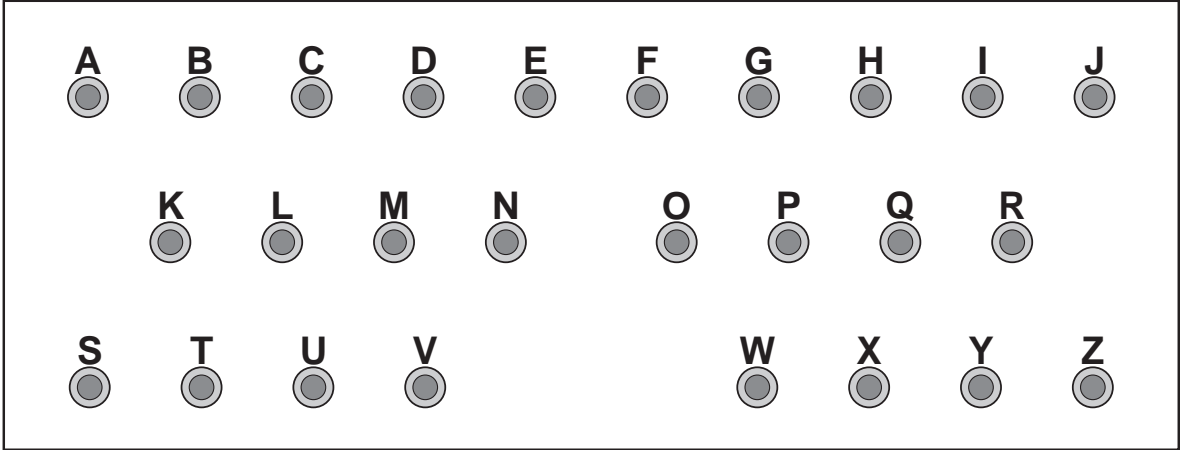
Overhead Slides

Overhead Slides

- 20.1 Plugboard
 - 20.2 Formula for Choosing m Pairs for n Objects
 - 20.3 Number of Settings for Enigma Machine
 - 20.4 'Paper Enigma'
-

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 $m = 2$.

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

$$= \underline{\hspace{10em}}$$

$$=$$

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
1 H A 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 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	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 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	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 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	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 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	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 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	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 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	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 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	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 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	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 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	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 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	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 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	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 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	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 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	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 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	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 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	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 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	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 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	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 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!)