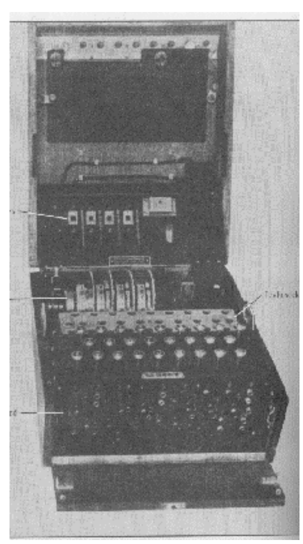
Lecture 3, Oct 1, 2001

- Enigma
- Algebraic Structures
- Projects

Enigma

Based on material by Fauzan Mirza <F.U.Mirza@sheffield.ac.uk>



Enigma

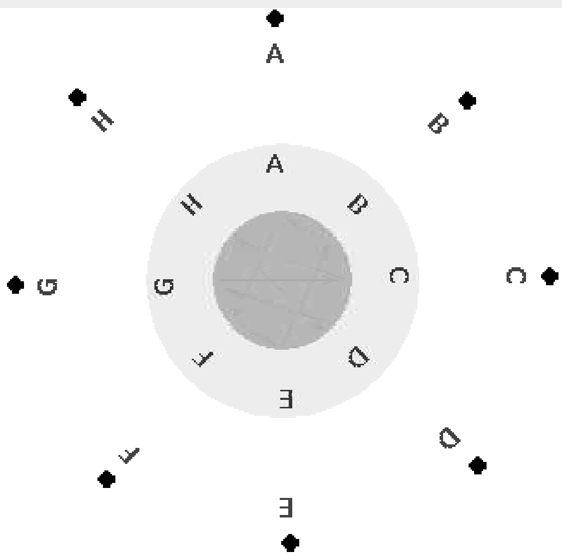
The algorithm combines 3 separate encryption stages:

- The plugboard (PL)
- The main rotors (MR)
- The reflecting rotor (RR)

p -> PL -> MR -> RR -> MR-1 -> PL -> c

The Main Rotors: the most complex part of the algorithm.

Enigma

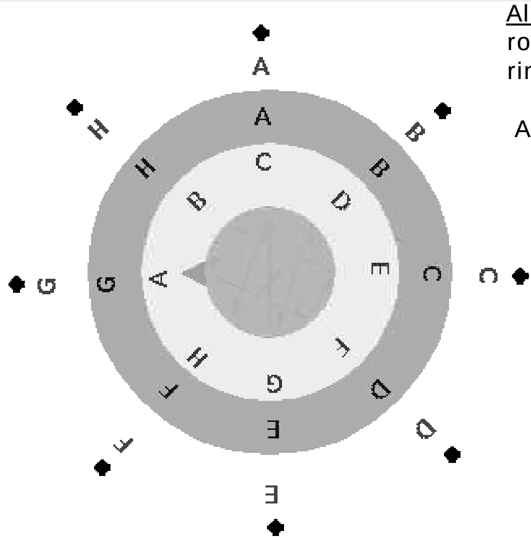


The Wired Map:

fixed monoalphabetic mapping. Note that letters "enter" and "exit" at the black dots, e.g.:

A -> F

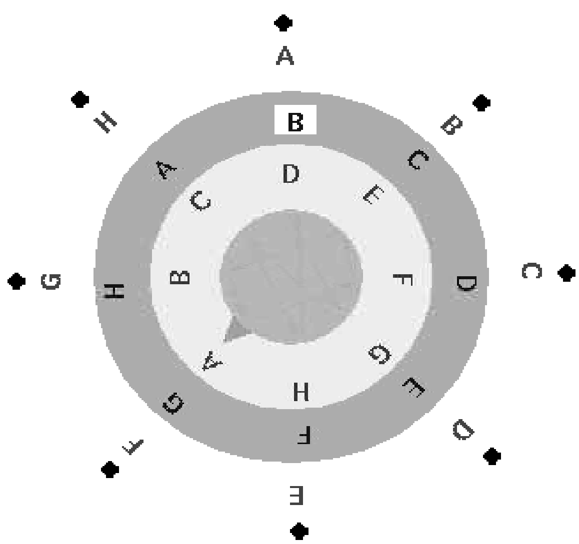
Enigma



<u>Alphabetic Ring:</u>The wired map is rotated with respect to an outer ring, e.g.:

A -> (wired C) -> (wired H) -> F

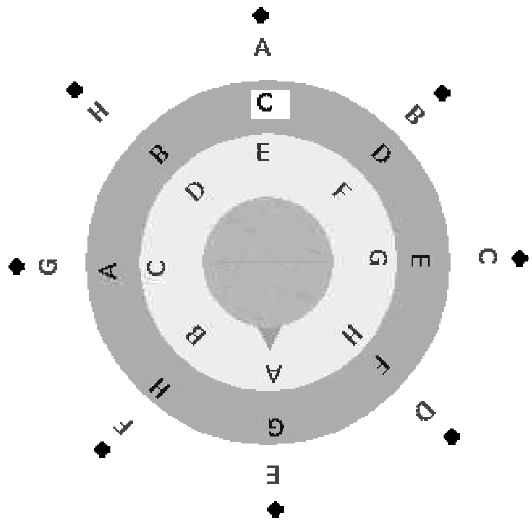
Enigma



<u>Rotor Window:</u>
The wired map and alphabetic ring rotate together with respect to input and output, e.g.:

a -> (rotated b) -> (wired d) -> (wired G) -> (rotated E) -> D

Enigma



The keys are:
- The ring position.
- The starting window position.

Rotation:
The rotor periodically rotates under the window, changing its shift

Enigma

Plugboard and reflecting rotor

The plugboard maps a few additional letters at the beginning and end.

The reflecting rotor is just a simple fixed transformation.

Putting it together

The machine used 3 rotors. The order of the rotors was part of the key.

The first selected rotor rotates on each letter. It has one fixed position ("rotor notch") at which it triggers the second rotor to rotate (once per revolution of the first). Similarly, the second has a position at which it triggers the third.

An Example:

Rotor wirings:

Input:	ABCDEFGHIJKLMNOPQRSTUVWXYZ
1:	EKMFLGDQVZNTOWYHXUSPAIBRCJ
2:	AJDKSIRUXBLHWTMCQGZNPYFVOE
3:	BDFHJLCPRTXVZNYEIWGAKMUSQO
4:	ESOVPZJAYQUIRHXLNFTGKDCMWB
5:	VZBRGITYUPSDNHLXAWMJQOFECK
R:	YRUHQSLDPXNGOKMIEBFZCWVJAT

Rotor notches:
1: Q
2: E
3: V
4: J
5: Z

Key

Rotor order:	3 1 2
Alphabet ring setting:	W X T
Rotor starting positions:	A W E
Plugboard:	(AM) (TE)

Enciphering "THISISATEST" using these settings

```
Input P    3      1      2     R      2      1      3    P  Output
  T   E [FJTPO][KNWTX][BIXQM] (MO) [SZSLH][DGFCG][HLFBA] A     M
  H   H [JNNJH][DGDAE][IPCVR] (RB) [FMOHD][ZCYVZ][BFCYW] W     W
  I   I [LPEAX][TWBYC][GNTMI] (IP) [TAATP][LOMJN][QUWSP] P     P
  S   S [WABXT][PSSPT][XESLH] (HD) [HOYRN][JMCZD][HLFBX] X     X
  I   I [NRWSN][JMOLP][TAATP] (PI) [MTNGC][YBWTX][CGSOJ] J     J
  S   S [YCFBV][RUAXB][FMWPL] (LG) [KRGZV][RUROS][YCGCW] W     W
  A   M [TXSOH][DGDAE][IPCVR] (RB) [FMOHD][ZCYVZ][GKUQJ] J     J
  T   E [MQIEW][SVIFJ][NUPIE] (EQ) [UBJCY][UXQNR][ZDBXP] P     P
  E   T [CGCYP][LOYVZ][DKLEA] (AY) [CJBUQ][MPTQU][DHDZQ] Q     Q
  S   S [CGCYO][KNWTX][BIXQM] (MO) [SZSLH][DGFCG][QUWSI] I     I
  T   E [PTAWL][HKNKO][SZEXT] (TZ) [DKDWS][ORXUY][JNNJY] Y     Y
```

See: http://home.cern.ch/~frode/crypto/historical.html

(Mostly) Finite Algebraic Structures

- **Groups**
  - **Abelian**
  - **Cyclic**
  - **Generator**
  - **Group order**
- **Rings**
- **Fields**
- **Subgroups**
- **Euclidian Algorithm**
- **CRT**

GROUPs

DEFINITION:A set G and *operator* @, (G,@) is a **group** if:

CLOSURE: for all $x,y \in G$, $x @ y \in G$

ASSOCIATIVITY: for all $x,y,z \in G$, $(x@y)@z = x@(y@z)$

IDENTITY: $\exists$ $I \in G$ such that for all $x \in G$, $I@x = x$

INVERSE: for all $x \in G$, $\exists$ *inverse element* $x^{-1} \in G$ such that $x^{-1}@x = I$

DEFINITION: A group (G,@) is **ABELIAN** if:

COMMUTATIVITY: for all $x,y \in G$, $x@y=y@x$

Groups (contd)

DEFINITION:An element $g \in G$ is a **group generator** of group (G,@) if for all $x \in G$, $\exists i$ such that

$x = g^i$ = g@g@g@...@g (i times)

In other words, G=<g>

DEFINITION: A group (G,@) is **cyclic** if a group generator exists!

DEFINITION: Group **order** of a group (G,@) is **the size of set G**, i.e., |G| or #{G} or ord(G)

DEFINITION: Group (G,@) is **finite** if ord(G) is fixed.

Rings and Fields

DEFINITION:A structure (R,+,*) is a **ring** if (R,+) **is an abelian group** and:

***CLOSURE:** for all $x,y \in R$, $x * y \in R$

***ASSOCIATIVITY:** for all $x,y,z \in R$, $(x*y)*z = x*(y*z)$

***IDENTITY:** $\exists$ $I \in R$ such that for all $x \in R$, $I*x = x$

***COMMUTATIVITY:** for all $x,y \in R$, $x*y=y*x$

DISTRIBUTION: for all $x,y,z \in R$, $(x+y)*z = x*z + y*z$

DEFINITION: A structure (F,+,*) is a **field** if (F,+,*) **is a ring** and:

***INVERSE:** for all $x \in R$, $\exists$ *inverse element* $x^{-1} \in R$ such that $x^{-1}*x = I$

Examples: Integers under addition

G = **Z** = integers = { … -3, -2, -1, 0 , 1 , 2 …}

the group operator is "+", ordinary addition

- ❑ the integers are closed under addition
- ❑ the identity is 0
- ❑ the inverse of x is -x
- ❑ the integers are associative
- ❑ the integers are commutative (so the group is abelian)

Positive Integers under Exponentiation?

G = {0, 1, 2, 3…}

the group operator is "^", exponentiation

- ❑ closed under exponentiation
- ❑ the identity is 1, x^1=x
- ❑ the inverse of x is always 0, x^0=1
- ❑ the integers are NOT commutative,

x^y<>y^x (non-abelian)

- ❑ the integers are NOT associative,

(x^y)^z = x^(y^z)

Non-zero rationals under multiplication

$$G = \mathbf{Q} - \{0\} = \{a/b\} \text{ where } a,b \in \mathbf{Z}^*$$

the group operator is "*", ordinary multiplication

- If a/b, $c/d \in Q-\{0\}$, then $a/b * c/d = (ac/bd) \in Q-\{0\}$
- the identity is 1
- the inverse of a/b is b/a
- the rationals are associative
- the rationals are commutative (so the group is abelian)

Non-zero reals under multiplication

$$G = \mathbf{R} - \{0\}$$

the group operator is "*", ordinary multiplication

- If a, $b \in R-\{0\}$, then $a*b \in R-\{0\}$
- the identity is 1
- the inverse of a is $1/a$
- the reals are associative
- the reals are commutative (so the group is abelian)

Integers mod N under addition

G = $\mathbf{Z}^{+}_{\mathbf{N}}$ = integers mod N = {0 ... N-1}

the group operator is "+", modular addition

- the integers modulo N are closed under addition
- the identity is 0
- the inverse of x is -x (=N-x)
- addition is associative
- addition is commutative (so the group is **abelian**)

Integers mod p (prime) under multiplication

G = $\mathbf{Z}^{*}_{\mathbf{p}}$ =non-zero integers mod p = {1 ... p-1}

the group operator is "*", modular multiplication

- integers mod p are closed under *:
  because if GCD(x, p) =1 and GCD(y,p) = 1
  then GCD(xy,p) = 1
- the identity is 1
- the inverse of x is from Euclid's algorithm:
  ux + vp = 1 = GCD(x,p)
  so x^{-1} = u
  also x^{-1} = u = x^{p-2}
- * is associative
- * is commutative (so the group is abelian)

Z^*_N : positive integers mod N relatively prime to N

G = Z^*_N =non-zero integers mod N = {1 …,x,… n-1} such that gcd(x,N)=1

Group operator is "*", modular multiplication
Group order ord(Z^*_N) = number of integers **relatively prime** to N denoted by $\phi(N)$

- integers mod N are closed under multiplication:
  if GCD(x, N) =1 and GCD(y,N) = 1, GCD(x*y,N) = 1
- identity is 1
- inverse of x is from Euclid's algorithm:
  $ux + vN = 1 = GCD(x,N)$
  so $x^{-1} = u$ ($= x^{\phi(N)-1}$)
- multiplication is associative
- multiplication is commutative (so the group is abelian)

Non-abelian Groups: GL(2), 2x2 non-singular real matrices under matrix mult-n

$$GL(2) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix}, ad-bc \neq 0 \right\}$$

- if A and B are non-singular, so is AB
- the identity is I = $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} / (ad-bc)$$

- matrix multiplication is associative
- matrix multiplication is **not** commutative

Non-abelian Groups (contd)

$$\begin{bmatrix} 2 & 5 \\ 10 & 30 \end{bmatrix}^{-1} = \begin{bmatrix} 3 & -0.5 \\ -1 & 0.2 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 5 \\ 10 & 30 \end{bmatrix}\begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 11 & 20 \\ 60 & 110 \end{bmatrix}$$

$$\begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} 2 & 5 \\ 10 & 30 \end{bmatrix} = \begin{bmatrix} 56 & 165 \\ 22 & 65 \end{bmatrix}$$

What about positive integers under MOD operation?

Subgroups

DEFINITION: (H,@) is a **subgroup** of (G,@) if:

- H is a subset of G
- (H,@) is a group

Subgroup example

Let $(G,*)$, $G = Z^*_7 = \{1,2,3,4,5,6\}$
Let $H = \{1,2,4\} \pmod 7$

Note:
1. H is closed under multiplication mod 7
2. 1 is still the identity
3. 1 is 1 inverse, 2 and 4 are inverses of each other
4. associativity holds
5. commutativity holds (H is abelian)

Subgroup example

Let $(G,*)$, $G = R-\{0\}$ = non-zero reals
Let $(H,*)$, $Q-\{0\}$ = non-zero rationals

H is a subset of G and G,H are groups

Order of an element

Let **x** be an element of a (multiplicative) finite integer group G.The *order* of **x** is the smallest positive number k such that $\mathbf{x}^k = 1$

Notation: ord(x)

Order of an element

Example: Z^*_7: the multiplicative group modulo 7

Note: $Z^*_7 = Z_7$

$Z^*_7 = \{1,2,3,4,5,6\}$

ord(1) = 1 because $1^1 = 1$
ord(2) = 3 because $2^3 = 8 = 1$
ord(3) = 6 because $3^6 = 9^3 = 2^3 = 1$
ord(4) = 3 because $4^3 = 64 = 1$
ord(5) = 6 because $5^6 = 25^3 = 4^3 = 1$
ord(6) = 2 because $6^2 = 36 = 1$

Theorem (Lagrange)

$\Phi(n)$ - order of G_n^*
largest order of any element!

order of g : smallest m such that
$g^m \equiv 1 \bmod n$

Theorem (Lagrange): Let G be a multiplicative group of order n. For any g in G, ord(g) divides n.

COROLLARY 1:
$b^{\Phi(n)} \equiv 1 \bmod n \;\forall\; b \in Z_n^*$
because : $\Phi(n) = \mathrm{ord}(Z_n^*)$
$ord(b) = \mathrm{ord}(Z_n^*)/k = \Phi(n)/k$
thus : $b^{\Phi(n)} = b^{\Phi(n)/k} = 1^{1/k} = 1$

COROLLARY 2:
if p is prime then
$\forall\; b \in Z_p^*$
1) $b^p \equiv b \bmod p$
and
2) $\exists\; a \in Z_p \ni ord(a) = p-1$
a – primitive element

Primitive Example

p=13, primitive elements={2,6,7,11}

Projects

Last Winter Projects:

- **Survey of Copy Protection and Watermarking**
- **A prototype group signature scheme**
- **A Survey of Digital Watermarking**
- **Knapsack Cryptosystems: Past, Present and Future**
- **A Secure FTP Client Prototype**
- **A Survey of Cryptography Research at KTH**
- **A Program to perform cryptanalysis of Vigenere**
- **A Multi-Party Non-repudiation Protocol**
- **A PCS Secure Communication Architecture**
- **An Analysis of Well-Known Secret Sharing Methods**
- **An Implementation of IPSec with Literate Programming**