Enigma

Enigma

- Developed and patented (in 1918) by Arthur Scherbius
- Many variations on basic design
- Eventually adopted by Germany
  - For both military and diplomatic use
  - Many variations used
- Broken by Polish cryptanalysts, late 1930s
- Exploited throughout WWII
  - By Poles, British, Americans

Enigma

- Turing was one of Enigma cryptanalysts
- Intelligence from Enigma vital in many battles
  - D-day **dis**information
  - German submarine "wolfpacks"
  - Many other examples
- May have shortened WWII by a year or more
- Germans never realized Enigma broken — Why?
  - British were cautious in use of intelligence
  - But Americans were less so (e.g., submarines)
  - Nazi system discouraged critical analysis…

Enigma

- To encrypt
  - Press plaintext letter, ciphertext lights up
- To decrypt
  - Press ciphertext letter, plaintext lights up
- Electo-mechanical

Enigma Crypto Features

- 3 rotors
  - Set initial positions
- Moveable ring on rotor
  - Odometer effect
- Stecker (plugboard)
  - Connect pairs of letters
- Reflector
  - Static "rotor"

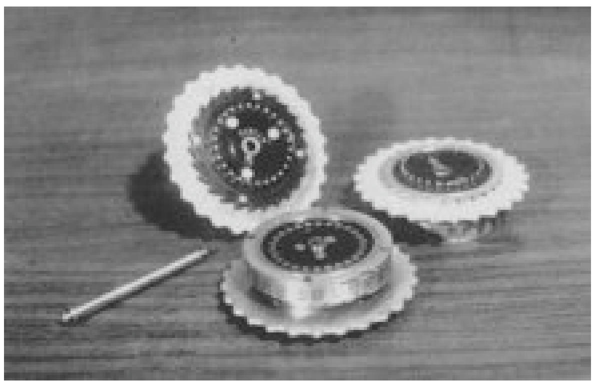
Substitution Cipher

- Enigma is a substitution cipher
- But not a simple substitution
  - Perm changes with each letter typed
- Another name for simple substitution is mono-alphabetic substitution
- Enigma is an example of a **poly-alphabetic substitution**
- How are Enigma "alphabets" generated?

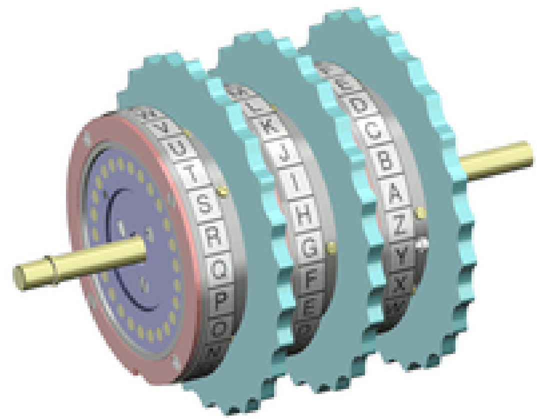
Enigma Components

- Each rotor implements a permutation
- The reflector is also a permutation
  - Functions like stecker with 13 cables
- Rotors operate almost like odometer
  - Reflector does not rotate
  - Middle rotor occasionally "double steps"
- Stecker can have 0 to 13 cables

Enigma Rotors



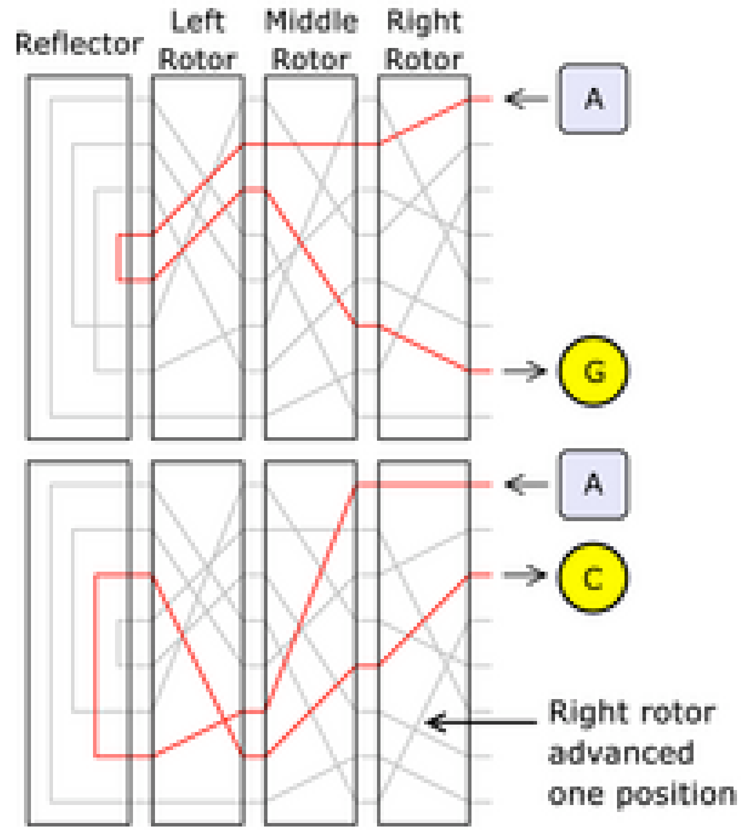
- Three rotors



- Assembled rotors

Rotors and Reflector

- Each rotor/reflector is a permutation
- Overall effect is a permutation
- Due to odometer effect, overall permutation changes at each step

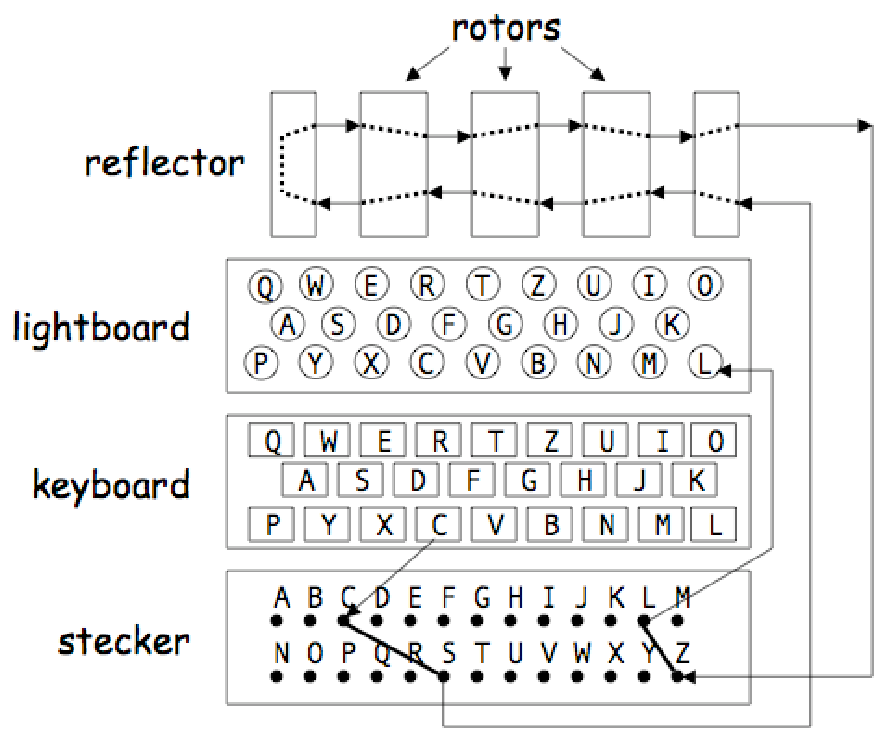


Why Rotors?

- Inverse permutation is easy
  - Need inverse perms to decrypt!
  - Pass current thru rotor in opposite direction
- Can decrypt with same machine
  - Maybe even with the same settings…
- Rotors provide easy way to generate large number of permutations mechanically
- Otherwise, each perm would have to be wired separately (as in Purple cipher…)

Wiring Diagram

- Enter C
- Stecker: C to S
- S permuted to Z by rotors/reflector
- Stecker: Z to L
- L lights up



Enigma is Its Own Inverse!

- Suppose at step i, press X and Y lights up
  - Let A = permutation thru reflector
  - Let B = thru leftmost rotor from right to left
  - Let C = thru middle rotor, right to left
  - Let D = thru rightmost rotor, right to left
- Then $Y = S^{-1}D^{-1}C^{-1}B^{-1}ABCDS(X)$
- Where "inverse" is thru the rotor from left to right (inverse permutation)
- Note: reflector is its own inverse
  - Only one way to go thru reflector

Inverse Enigma

- Suppose at step i, we have
  $Y = S^{-1}D^{-1}C^{-1}B^{-1}ABCDS(X)$
- Then at step i
  $X = S^{-1}D^{-1}C^{-1}B^{-1}ABCDS(Y)$
- Since $A = A^{-1}$
- Why is this useful?

Enigma Key?

- What is the Enigma key?
  - Machine settings
- What can be set?
  - Choice of rotors
  - Initial position of rotors
  - Position of movable ring on rotor
  - Choice of reflector
  - Number of stecker cables
  - Plugging of stecker cables

Enigma Keyspace

- Choose rotors
  - $26! \cdot 26! \cdot 26! = 2^{265}$
- Set moveable ring on right 2 rotors
  - $26 \cdot 26 = 2^{9.4}$
- Initial position of each rotor
  - $26 \cdot 26 \cdot 26 = 2^{14.1}$
- Number of cables and plugging of stecker
  - Next slide
- Choose of reflector
  - Like stecker with 13 cables…
  - …since no letter can map to itself

Enigma Key Size

- Let F(p) be ways to plug p cables in stecker
  - Select 2p of the 26 letters
  - Plug first cable into one of these letters
  - Then 2p - 1 places to plug other end of 1st cable
  - Plug in second cable to one of remaining
  - Then 2p - 3 places to plug other end
  - And so on…
- $F(p) = \text{binomial}(26,2p) \cdot (2p-1) \cdot (2p-3) \cdot \cdots \cdot 1$

Enigma Keys: Stecker

F(0) = 1
F(1) = 325
F(2) = 44850
F(3) = 3453450
F(4) = 164038875
F(5) = 5019589575
F(6) = 100391791500
F(7) = 1305093289500
F(8) = 10767019638375
F(9) = 53835098191875
F(10) = 150738274937250
F(11) = 205552193096250
F(12) = 102776096548125
F(13) = 7905853580625

F(0) + F(1) + … + F(13) = 532985208200576 = $2^{48.9}$

- Note that maximum is with 11 cables
- Note also that F(10) = $2^{47.1}$ and F(13) = $2^{42.8}$

Enigma Keys

- Multiply to find total Enigma keys
  $2^{265} \cdot 2^{9.4} \cdot 2^{14.1} \cdot 2^{48.9} \cdot 2^{42.8} = 2^{380}$
- "Extra" factor of $2^{14.1}$
  $2^{265} \cdot 2^{9.4} \cdot 2^{48.9} \cdot 2^{42.8} = 2^{366}$
- Equivalent to a 366 bit key!
- Less than $10^{80} = 2^{266}$ atoms in observable universe!
- Unbreakable? Exhaustive key search is certainly out of the question…

In the Real World (ca 1940)

- 5 known rotors: $5 \cdot 4 \cdot 3 = 2^{5.9}$
- Moveable rings on 2 rotors: $2^{9.4}$
- Initial position of 3 rotors: $2^{14.1}$
- Stecker usually used 10 cables: $2^{47.1}$
- Only 1 reflector, which was known: 2^{0}
- Number of keys "only" about

  $2^{5.9} \cdot 2^{9.4} \cdot 2^{14.1} \cdot 2^{47.1} \cdot 2^{0} = 2^{76.5}$

In the Real World (ca 1940)

- Only about $2^{76.5}$ Enigma keys in practice
- Still an astronomical number
  - Especially for 1940s technology
- But, most of keyspace is due to stecker
- If we ignore stecker…
  - Then only about 2^{29} keys
  - This is small enough to try them all
- Attack we discuss "bypasses" stecker

Enigma Attack

- Many different Enigma attacks
  - Most depend on German practices…
  - …rather than inherent flaws in Enigma
- Original Polish attack is noteworthy
  - Some say this is greatest crypto success of war
  - Did not know rotors or reflector
  - Were able to recover these
  - Needed a little bit of espionage…

Enigma Attack

- The attack we discuss here
  - Assumes rotors are known
  - Shows flaw in Enigma
  - Requires some known plaintext (a "crib" in WWII terminology)
  - Practical today, but not quite in WWII

Enigma Attack

- Suppose we have known plaintext (crib) below

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Plaintext	O	B	E	R	K	O	M	M	A	N	D	O	D	E	R	W	E	H	R	M	A	C	H	T
Ciphertext	Z	M	G	E	R	F	E	W	M	L	K	M	T	A	W	X	T	S	W	V	U	I	N	Z

- Let P_i be permutation (except stecker) at step i
- S is stecker
  - $M = S^{-1} P_8 S(A) \Rightarrow S(M) = P_8 S(A)$
  - $E = S^{-1} P_6 S(M) \Rightarrow S(E) = P_6 S(M)$
  - $A = S^{-1} P_{13} S(E) \Rightarrow S(A) = P_{13} S(E)$
- Combine to get "cycle" $P_6 P_8 P_{13} S(E) = S(E)$

Enigma Attack

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Plaintext	O	B	E	R	K	O	M	M	A	N	D	O	D	E	R	W	E	H	R	M	A	C	H	T
Ciphertext	Z	M	G	E	R	F	E	W	M	L	K	M	T	A	W	X	T	S	W	V	U	I	N	Z

- Also find the cycle
  - $E = S^{-1} P_3 S(R) \Rightarrow S(E) = P_3 S(R)$
  - $W = S^{-1} P_{14} S(R) \Rightarrow S(W) = P_{14} S(R)$
  - $W = S^{-1} P_7 S(M) \Rightarrow S(W) = P_7 S(M)$
  - $E = S^{-1} P_6 S(M) \Rightarrow S(E) = P_6 S(M)$
- Combine to get $P_6 P_{14}^{-1} P_7 P_6^{-1} S(E) = S(E)$

Enigma Attack

- Guess one of 2^{29} settings of rotors
  - Then all putative perms P_i are known
- If guess is correct cycles for S(E) hold
  - If incorrect, only 1/26 chance a cycle holds
- But we don't know S(E)
  - So we guess S(E)
- For correct rotor settings and S(E),
  - All cycles for S(E) must hold true

Enigma Attack

- Using only one cycle in S(E), must make 26 guesses and each has 1/26 chance of a match
  - On average, 1 match, for 26 guesses of S(E)
  - Number of "surviving" rotor settings is about 2^{29}
- But, if 2 equations for S(E), then 26 guesses for S(E) and only $1/26^2$ chance **both** cycles hold
  - Reduce possible rotor settings by a factor of 26
  - With enough cycles, will have only 1 rotor setting!
  - In the process, stecker (partially) recovered!
- Divide and conquer!

Bottom Line

- Enigma was ahead of it's time
- Weak, largely due to combination of "arbitrary" design features
  - For example, right rotor is "fast" rotor
  - If left rotor is "fast", it's stronger
- Some Enigma variants used by Germans are much harder to attack
  - Variable reflector, stecker, etc.

Bottom Line

- Germans confused "physical security" and "statistical security" of cipher
  - Modern ciphers: statistical security is paramount
  - Embodied in Kerckhoffs Principle
- Pre-WWII ciphers, such as codebooks
  - Security depends on codebook remaining secret
  - That is, physical security is everything
- Germans underestimated statistical attacks

Bottom Line

- Aside…
- Germans had some cryptanalytic success
  - Often betrayed by Enigma decrypts
- In one case, **before** US entry in war
  - British decrypted Enigma message
  - German's had broken a US diplomatic cipher
  - British tried to convince US not to use the cipher
  - But didn't want to tell Americans about Enigma!

Bottom Line

- Pre-computers used to attack Enigma
- Most famous, were the
  - Polish "bomba", British "bombe"
  - Electro-mechanical devices
- British bombe, essentially a bunch of Enigma machines wired together
- Could test lots of keys quickly
- Noisy, prone to break, lots of manual labor