

The Enigma Crypto Machine

Bob Harris

Department of Computer
Science and Engineering

Penn State

Nov/3/2005

rsharris@bx.psu.edu

Introduction

- Crypto machine used in WWII by German Military
- Cracked by a variety of techniques by Poles and English
 - Most famously by Turing and the crew at Bletchley Park
 - But Polish cryptographers Rejewski, Zygalski, and Różycki cracked it earlier
- Secret not declassified until the 1970s

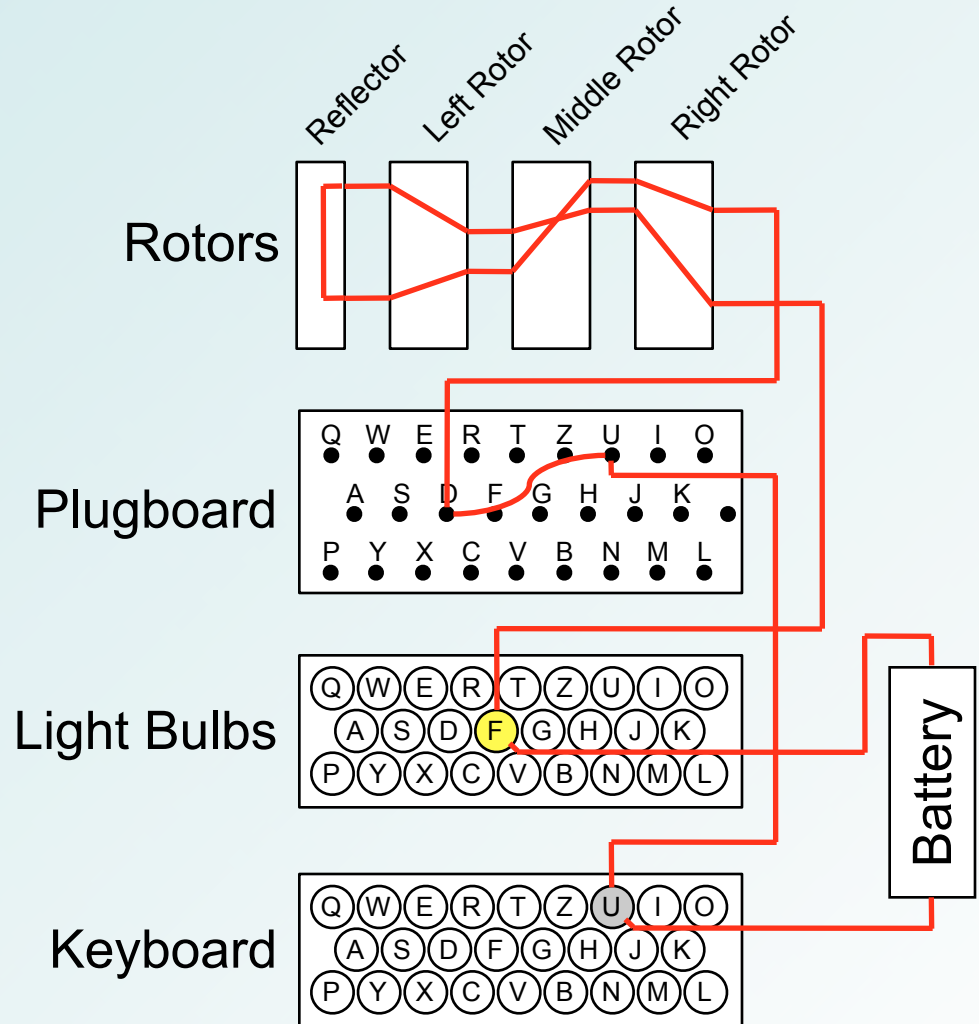


History

- Rotor-based crypto machines invented in many countries circa 1920
- Enigma's roots trace to patent by Koch, purchased and improved by Scherbius
- Scherbius targeted business communications
 - Sales brochure available, see [4]
- German military began using modified Scherbius design in late 1920s

How's It Work?

- Press plaintext U
- Mechanism moves rotors to next state
- Current rides through U wire to out of keyboard
- Plugboard shifts current to D wire
- Current rides on D wire to rotor bank
- Current rides the rotors, reflects, and comes out on F wire
- Bulb F lights
- Decrypt is the same, in reverse
 - Press F
 - U lights



Mechanical Details

- Rotors are wheels, with 26 spring-loaded pins on each side
- Internal wiring connects one pin from each side
 - Permutes the 26 possible signals, in both directions
- Reflector has pins only on one side, wires connect pairs
- Plugboard allows additional permutation (pair swaps)
- Gear mechanism advances rotors similar to odometer
 - Changes permutation for each letter encrypted or decrypted



Encryption Example

Message: Ich bin sicher, daß unser Führer eine lose Schraube hat

Plaintext: ICHBI NSICH ERDAS SUNSE RFUHR
EREIN ELOSE SCHRA UBEHA T

Cipher: OOFNH SEUKG ADIPP OJFLH ZZCPH
AXYLH SIUOS FSBGP KEWWS U

Try it yourself, using the default settings in this simulator:

http://homepages.tesco.net/~andycarlson/enigma/enigma_j.html

Changes From Original Design

- Early models actually printed message as a typewriter would
 - Removed to make the machine simpler for war manufacture?
- Early models also did not have the reflector
 - Current made one pass through the rotors
 - Decryption required a switch, to pass current through in the other order
- Adding the reflector actually added a weakness
 - No letter can be encrypted as itself
 - Set of permutations, with reflection, is a subgroup
- Early models had no plugboard
 - The plugboard is an improvement

More Design Choices

- Permutation inside rotors is irregular
 - Probably chosen at random
- Initially, all machines used the same three rotors
 - Simplifies distribution
 - Reduces manufacturing cost
 - Simplifies attacker's job
- Eventually added a 4th rotor
 - Narrow form factor to fit mechanics of existing units
- Rotor order can be changed
 - 6 orders for a 3 rotor machine
- Added 2 more rotors to the set
 - Choose any 3 of 5, 60 different ways
- Carry position on rotors can be adjusted

Key Space

- Key is initial setup of the machine
 - Rotor order
 - Plugboards
 - Rotor carry position (odometer mechanism)
 - Initial rotor letter settings
- $\approx 10^{22}$ different keys
- *Still, it's just a polyalphabetic cipher with a very large period*
 - Many keys give similar transformations
 - No transposition of the plaintext
- Frequency distribution is nearly uniform
 - Defeats attacks based on classical frequency analysis
 - But no letter can encrypt to itself

No Letter Encrypts to Itself

Cipher: OOFNH SEUKG ADIPP OJFLH ZZCPH AXYLH SIUOS FSBGP KEWWS U

Guess: UNSER FUHRE REINE LOSES CHRAU BEHAT

UNSE RFUHR EREIN ELOSE SCHRA UBEHA T

UNS ERFUH REREI NELOS ESCHR AUBEH AT

UN SERFU HRERE INELO SESCH RAUBE HAT

U NSERF UHRER EINEL OSESC HRAUB EHAT

UNSER FUHRE REINE LOSES CHRAU BEHAT

UNSE RFUHR EREIN ELOSE SCHRA UBEHA T

UNS ERFUH REREI NELOS ESCHR AUBEH AT

UN SERFU HRERE INELO SESCH RAUBE HAT

U NSERF UHRER EINEL OSESC HRAUB EHAT

UNSER FUHRE REINE LOSES CHRAU BEHAT

UNSE RFUHR EREIN ELOSE SCHRA UBEHA T

UNS ERFUH REREI NELOS ESCHR AUBEH AT

UN SERFU HRERE INELO SESCH RAUBE HAT

U NSERF UHRER EINEL OSESC HRAUB EHAT

UNSER FUHRE REINE LOSES CHRAU BEHAT

UNSE RFUHR EREIN ELOSE SCHRA UBEHA T

Cracking It

- Polish Secret Service (1928) had the foresight to begin working on it soon after Germany began using it
- Statistical analysis of intercepted cipher texts suggested the machine was a variant of the commercial Enigma
- They purchased the commercial version
- But they didn't know much else
 - Internal wiring of the rotors unknown
 - Existence of plugboard unknown
- French spies (1932) provided some details about German usage
 - Key distribution process
 - A couple months of expired daily key booklets

Key Distribution

- Germans distributed booklets showing the daily key settings
 - Operator sets plugboard, rotor order, carry position daily
 - Naval booklets (supposedly) printed with water soluble ink
- Sender chooses 3 letter message key K “at random”
 - Initial rotor letter settings
- Encrypt $K|K$ with daily key: $E_{\text{daily}}(K|K)$
- Set rotors to K
- Encrypt message
- Send $E_{\text{daily}}(K|K)|E_K(M)$
- This provides error correction for the message key
 - But it helps the attacker

Mathematical Model

- All components are permutations of the 26 letters
- Call the rightmost rotor N
- Call the combination of the other two rotors and the reflector Q
 - Assuming no carry, they behave as a unit
 - Note that Q must consist of 13 length-2 cycles
- The motion of first wheel is a known permutation P
 - Maps a to b, b to c, ...
- Call the plugboard S
 - Consists of only length-1 and length-2 cycles
- Another potential permutation H could exist between the the plugboard and the first rotor
 - Was used on some commercial machines
 - But (unknown to the Poles) not on the military one

Six Equations

- Assuming no odometer carry while encoding the message key (true for 77% of days), we have equations for the permutations for the first 6 letters
 - $A = SHPNP^{-1}QPN^{-1}P^{-1}H^{-1}S^{-1}$
 - $B = SHP^2NP^{-2}QP^2N^{-1}P^{-2}H^{-1}S^{-1}$
 - $C = SHP^3NP^{-3}QP^3N^{-1}P^{-2}H^{-1}S^{-1}$
 - $D = SHP^4NP^{-4}QP^4N^{-1}P^{-2}H^{-1}S^{-1}$
 - $E = SHP^5NP^{-5}QP^5N^{-1}P^{-2}H^{-1}S^{-1}$
 - $F = SHP^6NP^{-6}QP^6N^{-1}P^{-2}H^{-1}S^{-1}$
- The same permutations are used all day long, so if we intercept a lot of traffic perhaps we can figure them out
- Probably not (it's a hard problem). But we can gain some information to reduce the exhaustive search space.
- The first thing we know is all six permutations are their own inverses and consist of 13 cycles of length 2

Those First 6 Letters

- Plaintext for the first 6 letters is of the form $xyzxyz$
- Every intercepted message gives us $u=A(x)$ and $v=D(x)$
- Even without knowing x , we have
$$v = D(x) = D(A^{-1}(u)) = D(A(u)) = AD(u)$$
- So every intercepted message gives us an example of the combined permutations AD, BE, and CF
- With enough traffic, we can fully determine AD, BE, and CF
- This helps, but still not enough to solve the equations

Cycles + Guesswork = Message Keys

- Examining the cycles of AD is a clue
 - A permutation can be expressed as the composition of two permutations consisting of length-2 cycles if and only if it contains an even number of cycles of each length
 - For proof, see [3]
- This insight also yields a method for finding all the ways to decompose AD into A and D
- Typically reduces to $< 10,000$ possibilities for all six permutations
- This was reduced further by guessing that the keys weren't chosen at random
 - It turned out keys like WWW were common
- This is enough to determine the six permutations and recover message keys for all intercepts
 - Well, almost; a couple other guesses are needed

Determining the Rotors

- French had provided daily keys, so for this period S was known
- Another guess: H didn't really exist
 - Some sources claim instead that H was a simple permutation that was guessable
- The remaining equations can be solved to reveal N (see [3])
 - N is the rightmost rotor
- The intercepted daily keys turned out to cover two different rotors in the rightmost position
 - So two of the three rotors were solved this way
- Remaining rotor and reflector were easily determined

Built A Replica, Then What?

- By 1933 the Poles were able to build a functioning replica of the German Enigma
- Now they needed a method of recovering the daily key from new intercepts

Cracking the Daily Key

- Rightmost rotor
 - Statistical analysis of ciphertexts encrypted with similar message keys revealed where the carry mechanism moved the middle wheel
 - This was a unique property of each wheel, so it revealed which rotor was rightmost
- Plugboard settings
 - Plugboard doesn't change all letters
 - Print the 6 permutations A thru F
 - Print transformations of the form $V^{-x}NV^x$
 - Shift them along each other until observed correlations are matched
- Middle and Left rotor positions
 - Exhaustive search (1,352 trials)
 - Apparently this was performed manually

The Cyclometer

- Breaking message keys involved matching the cycle characteristics of the observed permutations AD, BE, and CF with those created by the settings of the rotors
- ≈ 1 million observed characteristics possible theoretically, but only ≈ 100 thousand could be produced by the machinery
 - Thus the observed characteristic would be sufficient to identify the settings of the rotors
- The Poles built an electromechanical machine to create a catalog of characteristics

Another Story

- Late in 1938, the Germans changed their key distribution scheme
 - Rendered previous cracking techniques obsolete
- Poles developed a machine called “Bomba”
 - The equivalent of 6 Enigmas being driven automatically
 - Could determine rotor positions in two hours
- In 1939, with war likely, the Poles passed their finding along to the French and British
- And that’s where this presentation ends

References

- [1] Gaj K, Orłowski A, “Facts and Myths of Enigma: Breaking Stereotypes”. Eurocrypt 2003: 106-122
- [2] Carlson A, “Simulating the Enigma Cypher Machine”.
http://homepages.tesco.net/~andycarlson/enigma/simulating_enigma.html
- [3] Tuma J, “Permutation Groups and the Solution of German Enigma Cipher”. 2003
<http://frode.home.cern.ch/frode/crypto/index.html>
- [4] “The Glow-Lamp Ciphering and Deciphering Machine” (Enigma Sales Brochure) Cryptologia Volume XXV, Number 3, July 2001, 161-173
<http://www.dean.usma.edu/math/pubs/cryptologia/ClassicArticleReprints/V25N3PP161-173EnigmaPamphlet.PDF>
- [X] Images, used with permission, from
<http://www.ilord.com/enigma.html>