Mathematics in Cryptography

Course Preview

Women and Mathematics Program 2018

Schedule & Setup

Course Outline

- **Day 1** – Engima: *The Beginning of Modern Cryptography*
- **Day 2** – Public Key Cryptography: *RSA, Diffie Hellman, and beyond*
- **Day 3** – Cryptography Meets the Internet: *SSL/TLS and HTTPS*
- **Day 4** – The Future: *Quantum Computing and Digital Cash*

Course Materials

Course packet

- Link will be shared via email.
- Contains exercises and supplementary information.

Code and data for exercises

- Will be shared via CoCalc.

Software Setup

Let's make sure everyone is ready to go!

Step 1

- Open your email to find the links to the course packet and CoCalc.

Step 2

- Follow the link to the course packet and go to Day 0: Course Setup. Install Wireshark as instructed.

Step 3

- Create your CoCalc account using the link emailed to you.

Step 4

- If you finish early, peruse the course packet to get a feel for the topics we will cover over the next few days!

Bits & Nibbles & Bytes & Hex

The bread and butter of cryptographers.

Base 10

Traditional integers are written in base 10.

Example: 27 = two 10s + seven 1s.

Example: 7389 = seven 1000s + three 100s + eight 10s + nine 1s.

Bits and Nibbles and Bytes

Humans think in 10s, but computers don't.

Binary is a way of representing integers using only 0s and 1s, which correspond to electrical pulses in a physical computer.

Bits and Nibbles and Bytes

Humans think in 10s, but computers don't.

Binary is a way of representing integers using only 0s and 1s, which correspond to electrical pulses in a physical computer.

0

bit

Bits and Nibbles and Bytes

Humans think in 10s, but computers don't.

Binary is a way of representing integers using only 0s and 1s, which correspond to electrical pulses in a physical computer.

1000

nibble

Bits and Nibbles and Bytes

Humans think in 10s, but computers don't.

Binary is a way of representing integers using only 0s and 1s, which correspond to electrical pulses in a physical computer.

1101 1000

byte

Base 2

Base 2 allows the representation of integers with bits.

Base 10	**Base 2**
0	$0 = 2^0*0$
1	$1 = 2^0*1$
2	$10 = 2^1*1 + 2^0*0$
3	$11 = 2^1*1 + 2^0*1$
4	$100 = 2^2*1 + 2^1*0 + 2^0*0$
5	$101 = 2^2*1 + 2^1*0 + 2^0*1$
6	$110 = 2^2*1 + 2^1*1 + 2^0*0$
7	$111 = 2^2*1 + 2^1*1 + 2^0*1$
8	$1000 = 2^3*1 + 2^2*0 + 2^1*0 + 2^0*0$

Base 2

Example: 27 = one 16 (2^4) + one 8 (2^3) + one 2 (2^1) + one 1 (2^0) = 11011.

Base 2

Challenge: represent 58 in base 2 notation.

Base 2

Challenge: represent 58 in base 2 notation.

Answer: 111010

Hex

Hex (or base 16) is an efficient way of representing binary integers.

Recall: one nibble = four bits.

One hex character encodes one nibble.

Hex character values are 0-9, a-f. For clarity, hex numbers always start with 0x.

Hex

Example: 451 = one 256 (16^2) + twelve 16s (16^1) + three 1s (16^0) = 0x1c3

Hex

Challenge: Convert 591983 to base 2 and hex.

Hex

Challenge: Convert 591983 to base 2 and hex.

Answer: base2 = 10010000100001101111, hex = 0x9086f

Enigma

A sneak peek.

Preview: Enigma

1923

Arthur Scherbius patents Enigma cipher machine.

1926

German Navy, Army, and Air Force begin using Engima machines.

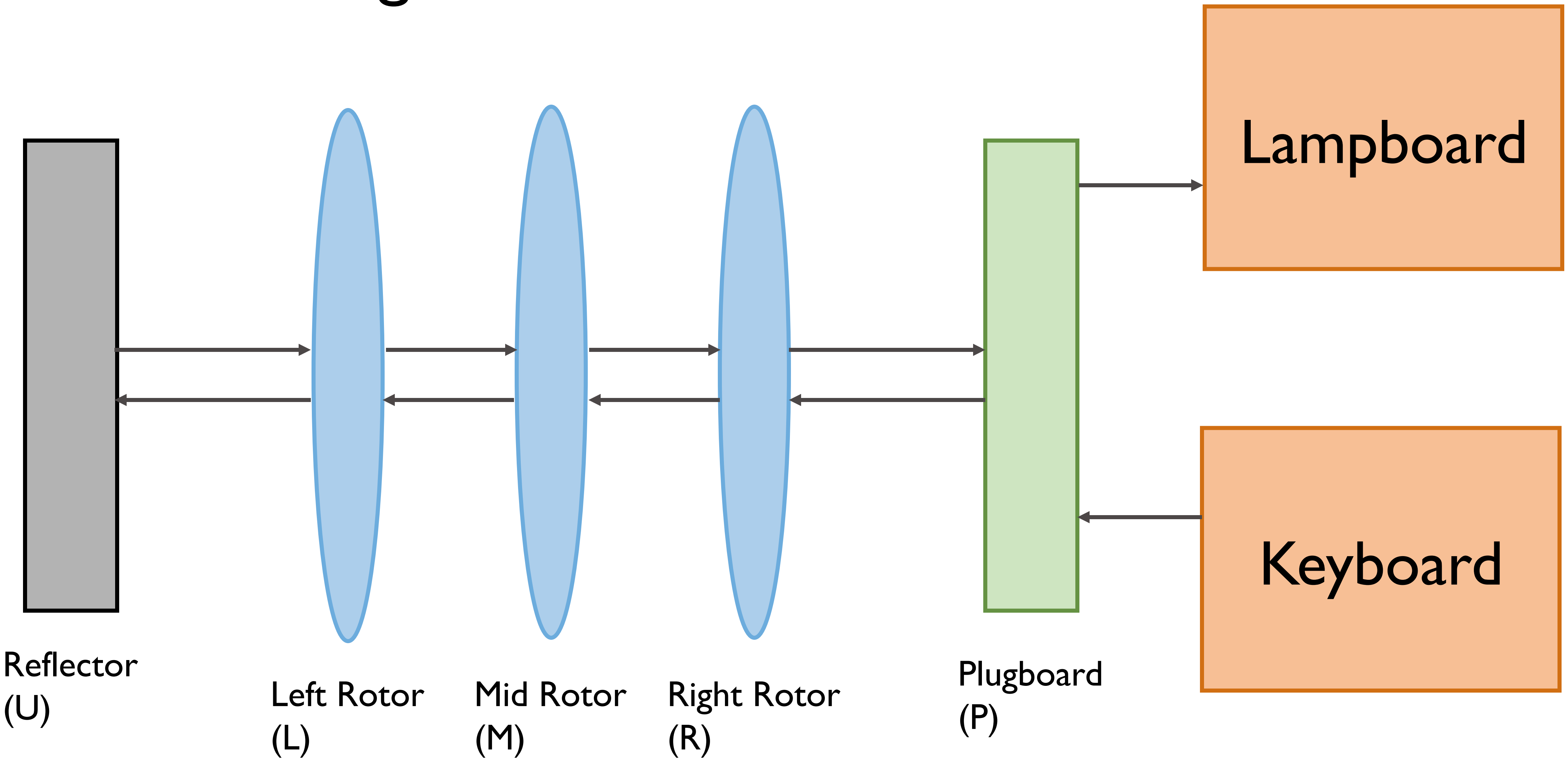
1932

Marian Rejewski at Polish Cipher Bureau invents first methods of cracking Enigma.

1940

Turing improves on Rejewski's methods to recover Enigma machine day key settings.

Preview: Enigma



Preview: Enigma

The Enigma transforms each keyboard letter with a set of permutations applied by the plugboard *P*, three rotors *L*, *M*, and *R*, and the reflector *U*. Mathematically, we can define this encryption E as:

$$E = PRMLUL^{-1}M^{-1}R^{-1}P^{-1}$$

Preview: Enigma

The rotation of the each rotor changes the encryption each time a key is pressed. If rotor *R* is rotated *i* positions, it now provides the transformation $p^i R p^{-i}$, where p is a cyclic permutation mapping A to B, B to C, etc.

Thus the whole encryption E can now be expressed as:

$$E = P\,(p^i R p^{-i})(p^j M p^{-j})(p^k L p^{-k})U(p^k L^{-1} p^{-k})(p^j M^{-1} p^{-j})(p^i R^{-1} p^{-i})P^{-1}$$

Questions?