Revising Cryptography: Again

Whitfield Diffie

Gonville and Caius College
Cambridge University

Vienna, Austria
6 June 2024

The Current Situation

- Quantum Computing seems to be progressing fast.
- It may threaten current public-key cryptography within decades or even years.
- NSA and NIST have proposed new "quantun-safe" systems.

We will look at the situation both in some detail and in historical context.

Cryptography

Transformation of comprehensible, usable information into incomprehensible, useless garbage (and back) under the control of secret keys.

Why Use Cryptography?

- No need to guard the message path.
- Can pass message through the hands of opponents.
- Cryptography acts like an amplifier.

Public-Key Cryptography

- Separate encryption and decryption capabilities
- Key negotiation
- Digital Signatures

Public-Key Cryptosystems

- RSA (Rivest, Shamir, Adelman)
- Diffie-Hellman key negotiation
- El Gamal signatures

Elliptic Curve Cryptography

- More complex arithmetic, smaller sizes
- Neal Koblitz and Victor Miller
- Elliptic Curve Diffie-Hellman and El Gamal

NSA Suite B: 16 February 2005

- Advanced Encryption Standard
- SHA-256 and SHA-384
- Elliptic Curve Diffie-Hellman
- Elliptic Curve DSA

Along Comes Quantum Computing

- Superly parallel
- Promised for thirty years and counting
- Rapidly developing
- Will break current public-key systems

How Does Quantum Computing Break Public-Key Crypto?

- In a public-key system, anyone can do the forward operation.
- It is going back that is hard.

The Secret in RSA

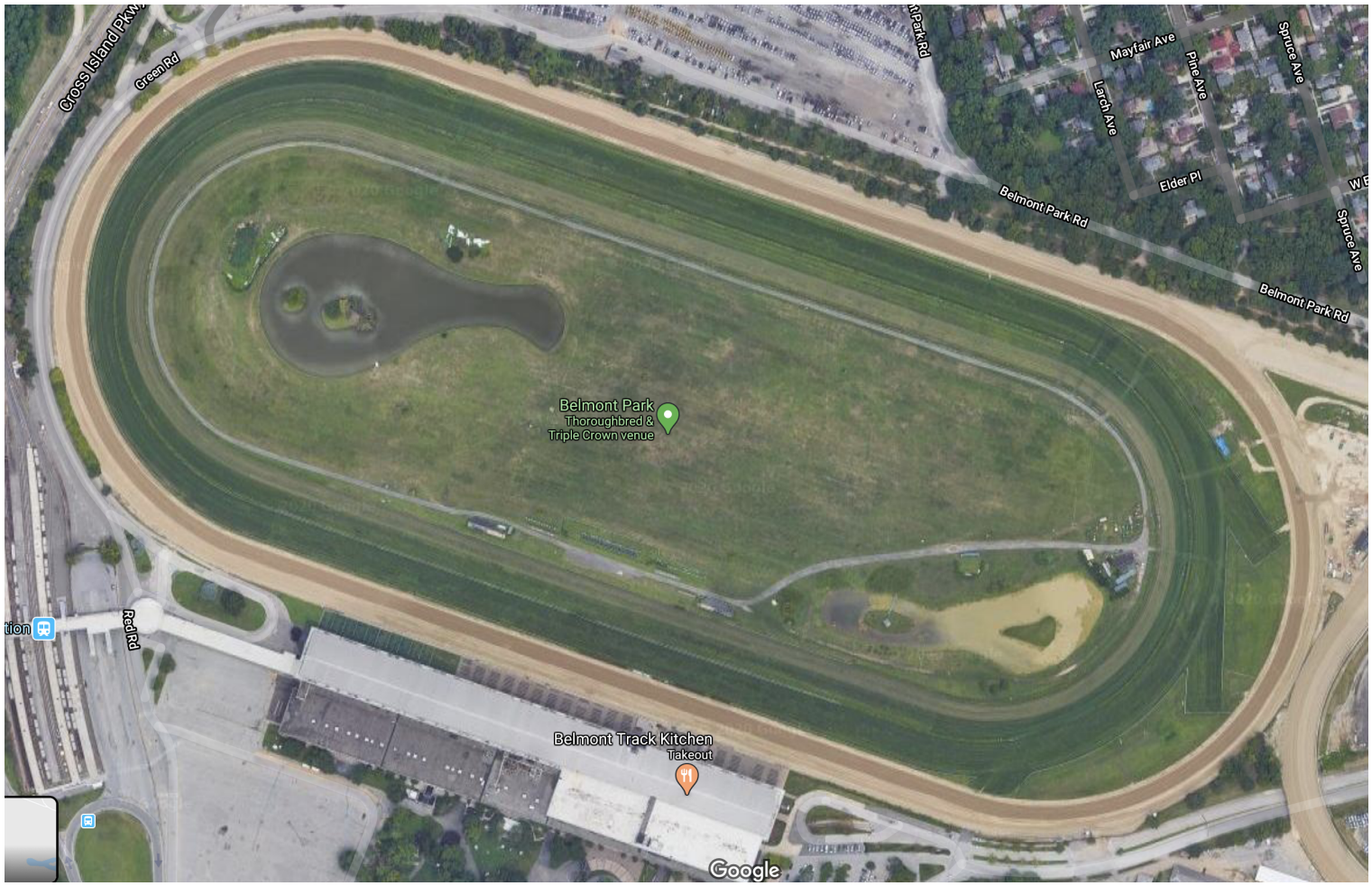
- Factors?

  Alternateively

- Length of a cycle $(p-1)(q-1)$

The step just before where you are is the decryption of what you started with.

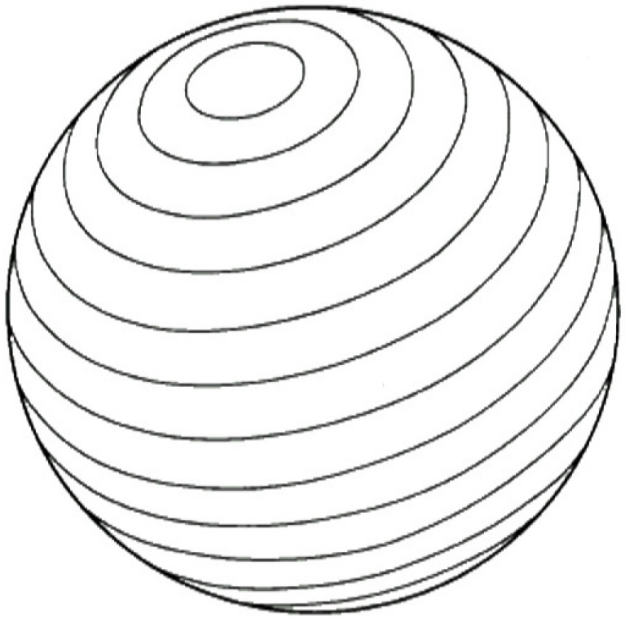
Like a Race Track



You Can't Go Back

Like moving on a track, if you go forward long enough, you will get back where you started.

In systems like Diffie-Hellman and RSA, it is easy to move a long way forward very quickly.



You went all the way around a cycle but how long is the cycle? How far do you go? That's the big secret.

Shor's Algorithm

Finds cycle length.

It will tell you how far to go.

Breaks the currently-used public key systems.

What to Do?

CNSS Advice 11 August 2015

IAD recognizes that there will be a move, in the not distant future, to a quantum resistant algorithm suite. ... For those partners and vendors that have not yet made the transition to Suite B algorithms, we recommend not making a significant expenditure to do so at this point ...

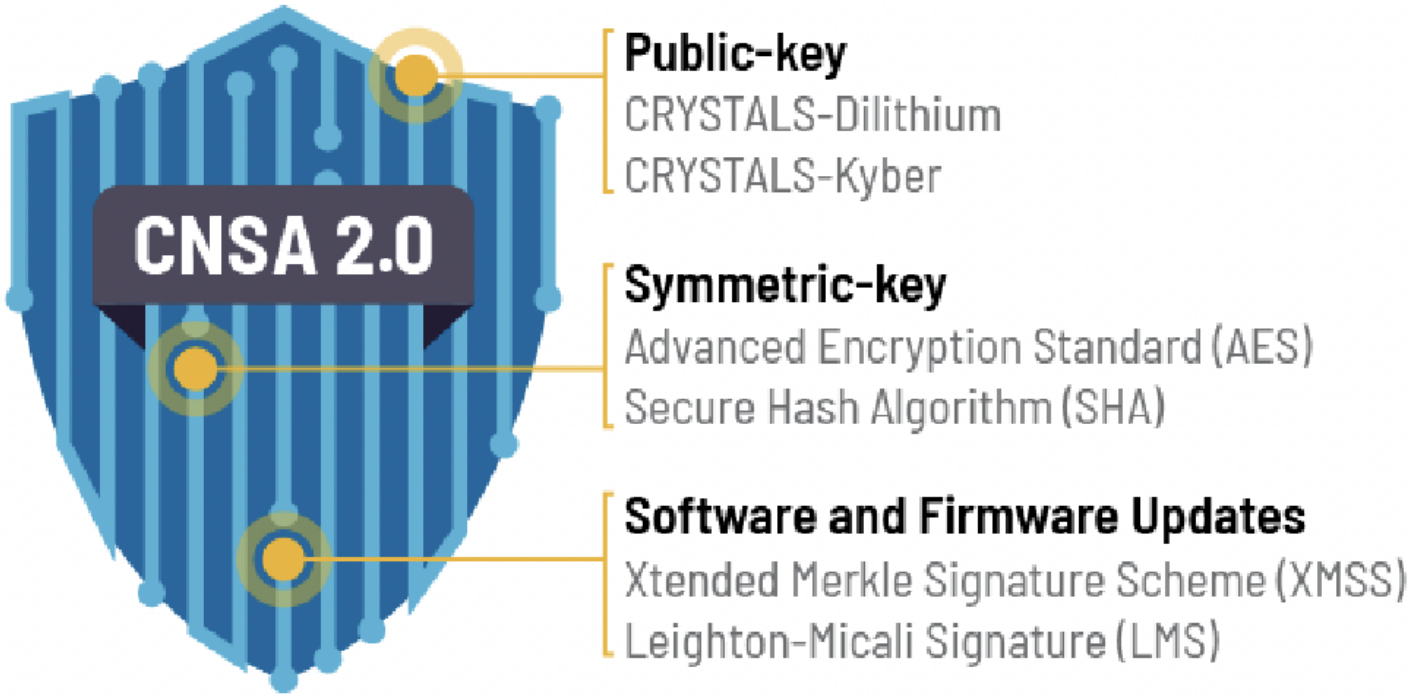
NIST: 5 July 2022
New Standards

- Key establishment
  - CRYSTALS-Kyber
- Digital signature
  - CRYSTALS-Dilithium (recommended)
  - Falcon
  - SPHINCS+

Are the New Systems Safe?

- Largely lattice-based
- Yilei Chen, "Quantum Algorithms for Lattice Problems"
- Withdrawn but Shamir is optimistic

Commercial National Security Algorithm Suite 2.0



People Think It's All New

- Collect (Harvest) now
- Exploit (Decrypt) later

Happening at least since WWI

Historical Context

Every generation or so, cryptography goes through a big transition, caused by new requirements and new techniques. Quantum computing is the current one; there have been several; and there will be more.

Elements of Change

- New challenges
- New techniques

"Modern" Cryptography Was Conceived Twice

- 200AH—Al Kindi in Baghdad
- 1500AD—Alberti et al. in Italy

- The basic ideas are not new.

Basic Ideas

- Polyalphabetic Ciphers: substitution must change from character to character
- Techniques: arithmetic and table lookup

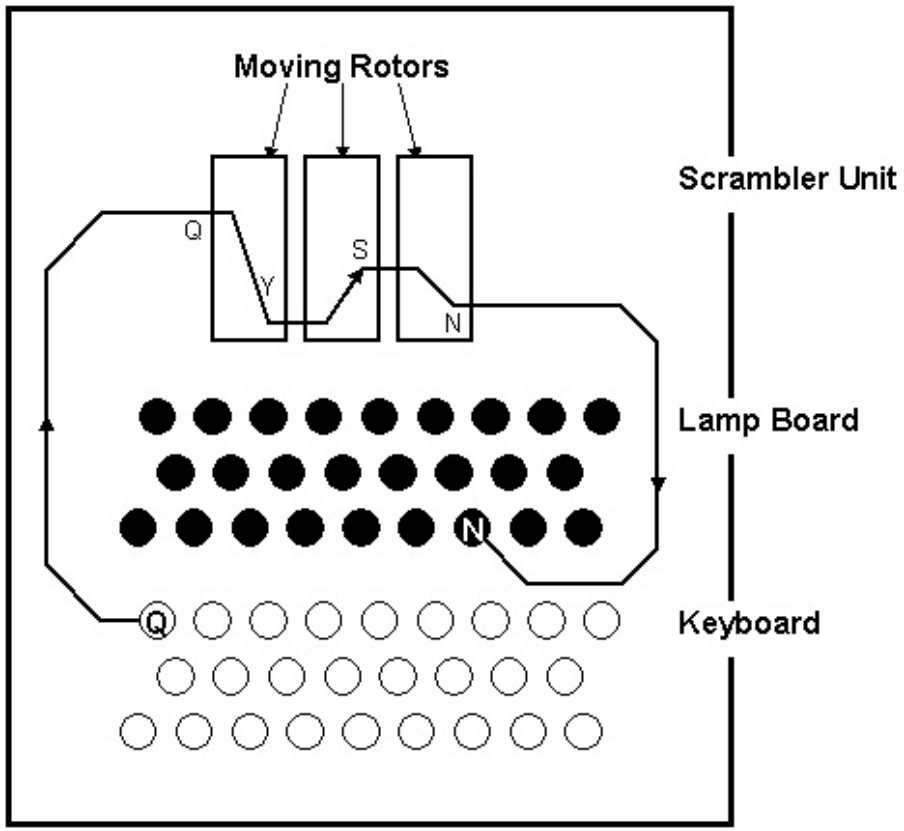
- Q: Why was cryptography so slow to develop?
- A: You can't really do it without machine computing.

World War I
Birth of Modern Cryptography

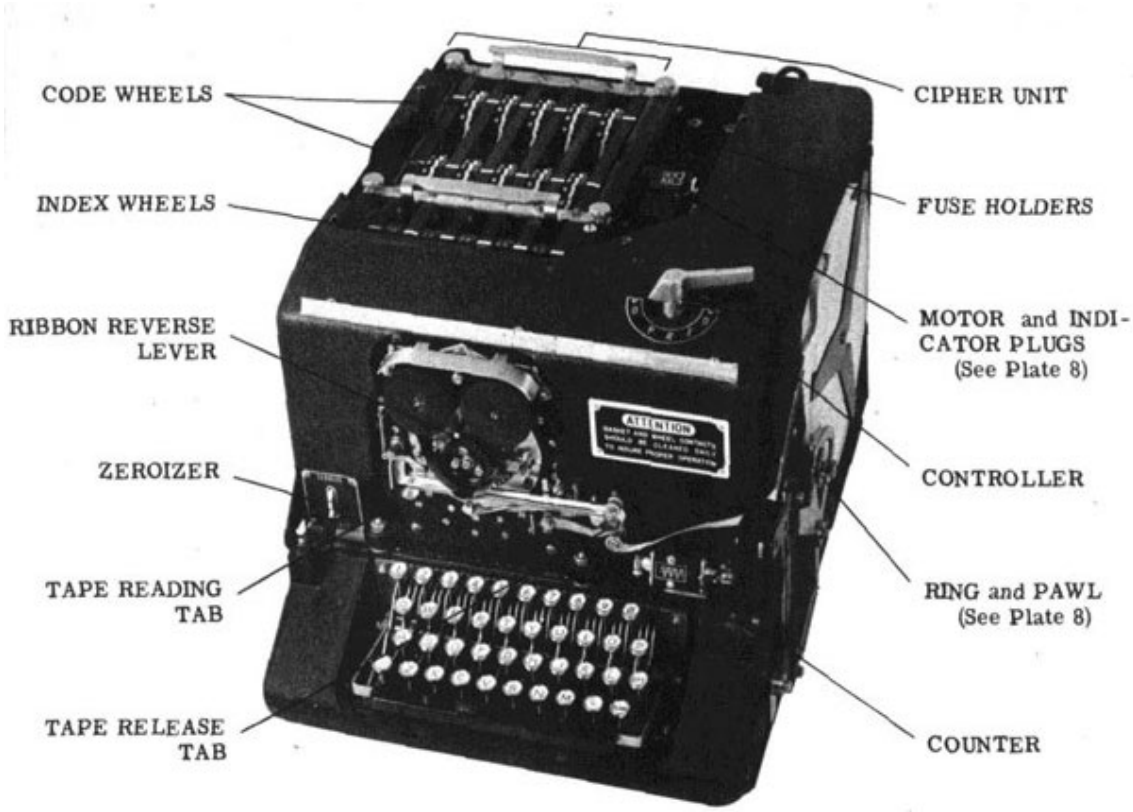
- Challenge: Radio
- Techniques: Machining and Electricity

Rotor

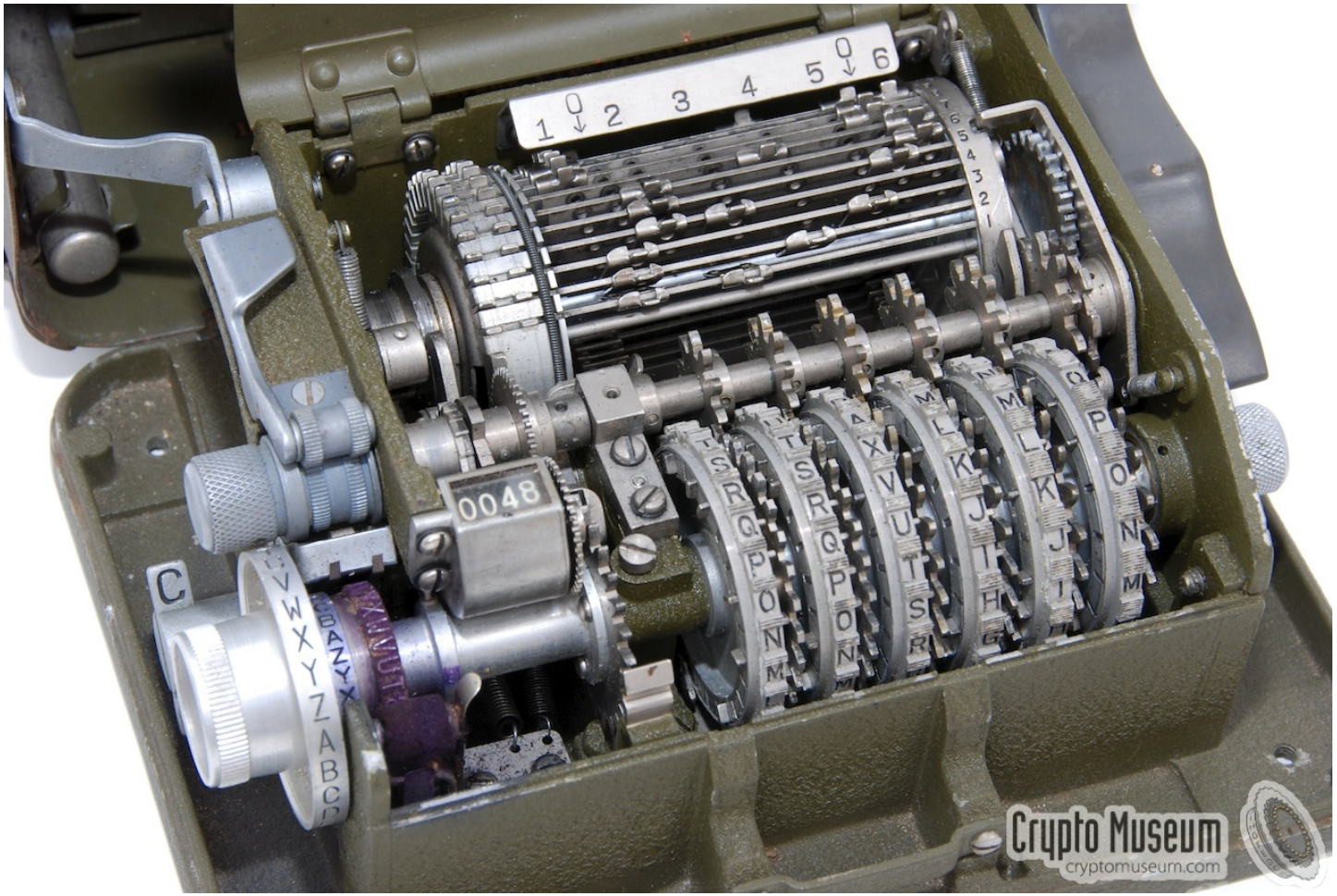
Rotor Encryption



Sigaba


CODE WHEELS
INDEX WHEELS
RIBBON REVERSE LEVER
ZEROIZER
TAPE READING TAB
TAPE RELEASE TAB
CIPHER UNIT
FUSE HOLDERS
MOTOR and INDICATOR PLUGS (See Plate 8)
CONTROLLER
RING and PAWL (See Plate 8)
COUNTER

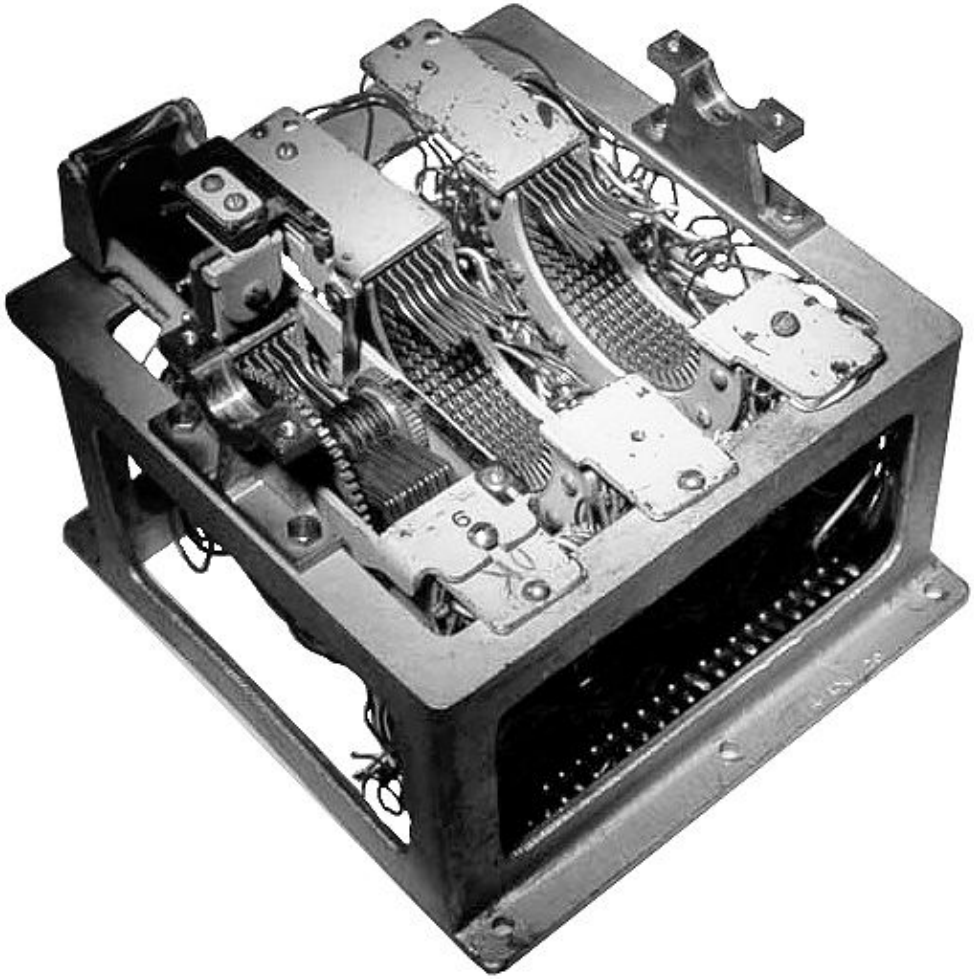
Pinwheel Machines



Japanese Type 97 (Purple)

The Japanese Type 97 system, which the U.S. called Purple, was made of stepping switches, available, non-custom, parts.

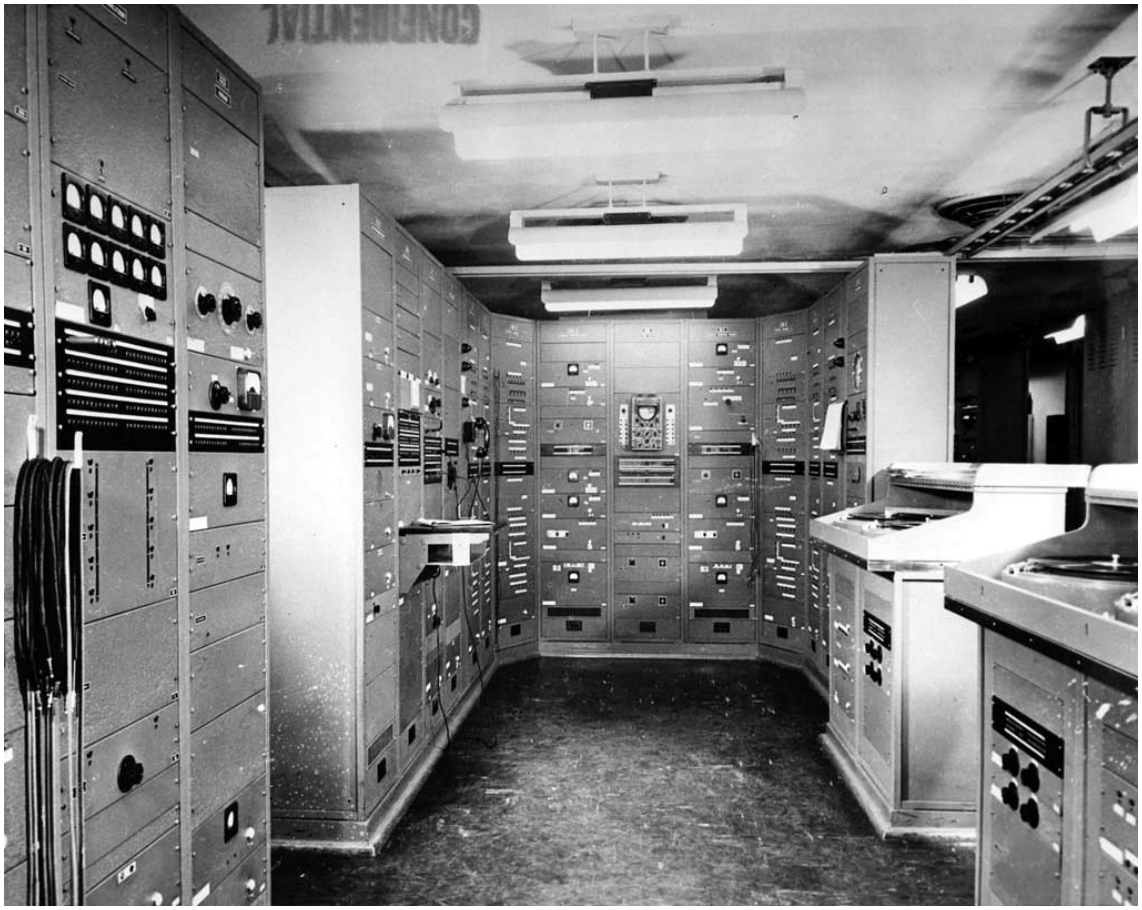
Japanese Type 97 (Purple)



World War II
Rise of Electronics

- Challenge (hard to hide):
  traffic volume
- Challenge (secret): Computing
- New technique: Electronics

Sigsaly



World's first digital telephone

Many Elements Over a 30-Year Period

- Custom Electronics (shift registers)
- Computer-like machines
- Stream ciphers go to block ciphers
- Cryptography in software

Late 20th Century Change of Scale

- Birth of the Internet
- Cryptography Goes Public
- Computing gets cheap
- Public-key cryptography

Early 21st Century Quantum Computing

- Challenge: Quantum Computing
- Techniques: New Cryptosystems

Late 21st Century
Who Knows

But we know it will happen