Exploration of Cryptography

Whitfield Diffie

Distinguished Visiting Professor

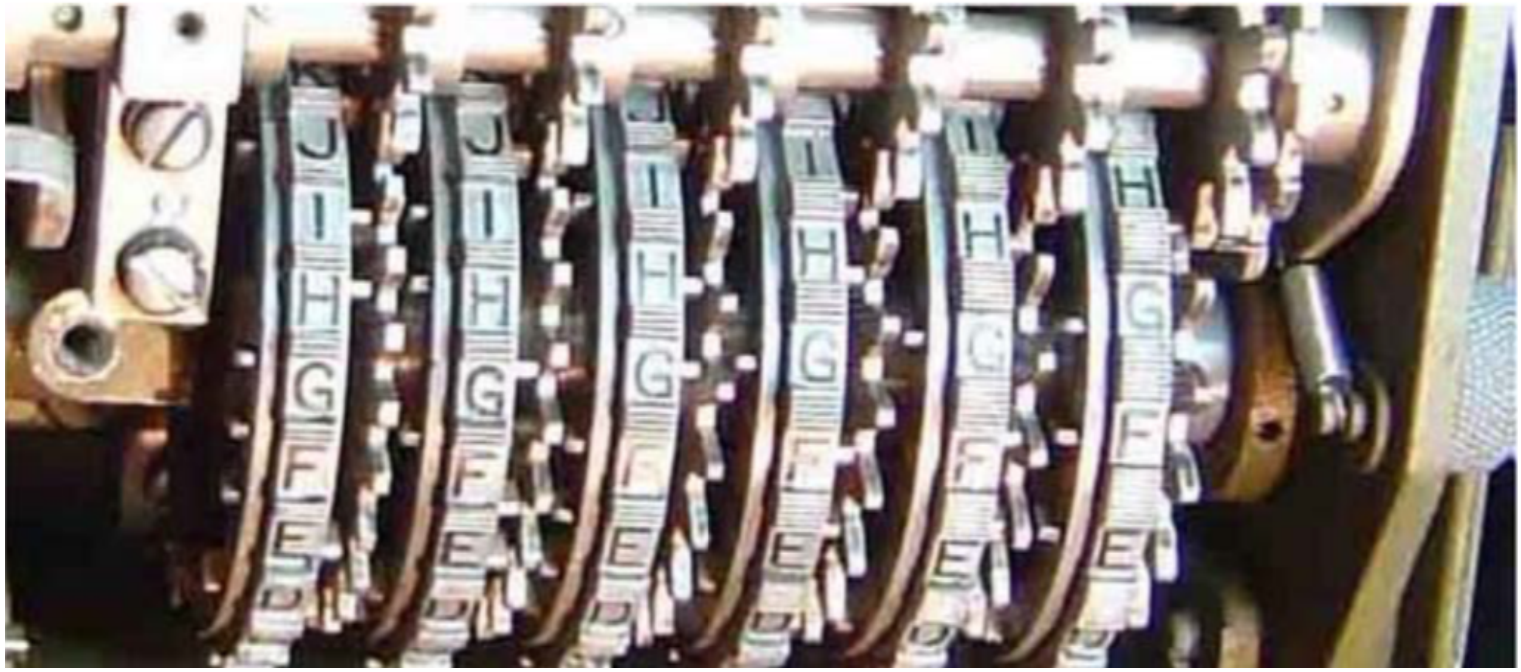
Zhejiang University

14 December 2020

Class 06
Homework and
Key Management

Homework 1
Pinwheel Machines
Rotor Machines
and Shift Registers

1 - Pinwheel Machine Periods



A pinwheel machine is a machine in which the known-period element is a set of wheels of various sizes, each of which presents a bit on its edge in each position it assumes. At each clock tick, each wheel steps 1 place. On the first wheel, note pins sticking left next to E, F, and G, right next to H and I, then left again next to J.

Suppose a pinwheel machine has n wheels of sizes (number of pins, i.e., bits) ℓ_1 through ℓ_n. Show that the machine has maximal period only if $\ell_1 \ldots \ell_n$ are relatively prime.

More generally, show that the period of the machine is

$$\text{lcm}\,(\ell_1 \ldots \ell_n)$$

2 - M-109

Consider a pinwheel machine with smaller and fewer wheels than the M-209, say of sizes 18, 17, 15, 13, and 11 for which the pin positions on each wheel are numbered 0 through $n - 1$.

What is the period of this machine?

Suppose that the pins on the wheels are set as follows:

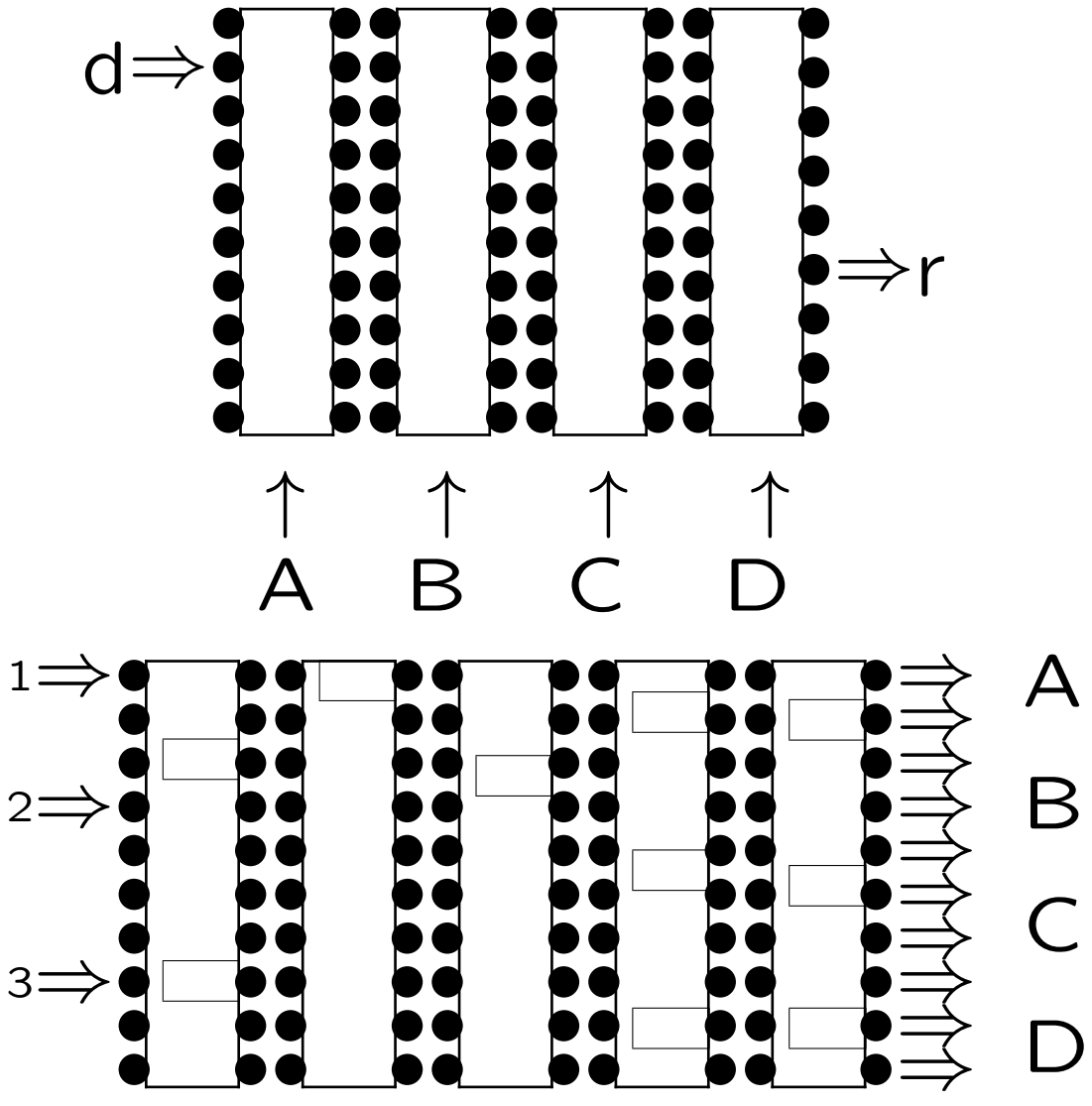
- 18: 1, 3, 5, 7, 9, 11, 13, 15, 17
- 17: 0, 1, 2, 3, 4, 5, 6, 7, 8
- 15: 7, 8, 9, 10, 11, 12, 13, 14
- 13: 2, 3, 4, 5, 6, 7, 8
- 11: 0, 2, 3, 5, 10

and that the machines starts (message indicator) in position: 6, 4, 13, 1, 9. That is to say that the first wheel has been rotated six from straight up, etc.

What is the 5-bit number that presents straight up?

What 5-bit number will present after the machine has stepped 2^{16} steps?

3 - Sigbubba



Consider a Sigaba-like machine, Sigbubba, with has two banks 16-character rotors. The lower bank are the control rotors and the upper bank are the cipher rotors. The lower bank has five rotors. These move in an odometer pattern except that wheel 1 (far right) is followed by wheel 3 (center) followed by wheel 5

(far left) followed by wheel 2 (between 1 and 3) and finally wheel 4 (between 3 and 5). (This motion pattern may or may not come up in some future problem.) The upper bank has only four rotors.

Three signals enter at the left end of the control rotors; their positions are

selectable. Four groups emerge on the right, each one being the "wire-or" of four emerging wires. Each of these groups will drive one of the cipher rotors.

- What is the expected fraction of the time that each wheel moves?

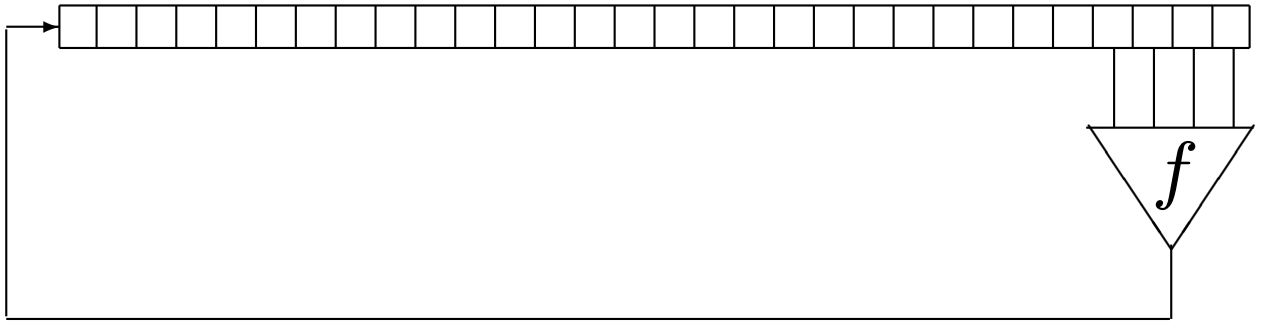
- What is the expected number of wheels that move at each clock tick?

4 - Sigbubba - bis

Since Sigbubba has four cipher rotors, there could be as many as 2^4 possible patters of motion that could occur.

- How many of these patters of motion actually occur?
- For all possible patterns of output from the control rotors, how often does each pattern occur?

5 - Nonlinear FSR



What must the structure of the function f be for the shift register to be invertible?

Key Management

Management View of Cryptography

- Crypto is an amplifier
- Separates security from path of message

Key management systems both reflect and shape the organizations that employ them.

Function of Key Management

Couples cryptography to bureaucracy:

clearances, ranks, jobs ...

Elements of Key Management

- Production
- Testing
- Shipping and Storage
- Use (to encrypt or decrypt)

Elements of Key Management (Cont'd)

- Accounting
- Destruction

Key Production

- There is no more critical crypto function
  - If you can produce good key, you have the possibility of good cryptoography.
  - If you can't, you don't.

Generating Unpredictability (Randomness)

- Card shuffling
- Rotors
- Slot machines
- Thermal noise
- Astable multivibrators
- Radioactive decay

Randomness (Cont'd)

- Atmospheric turbulence in Winchester disks
- Half-silvered mirror (ETH)
- Human variability

Desiderata

- Never seen by human eyes
  - Impossible with code books and rotors
- Failing that, secrecy of key, until traffic declassified.

Desiderata (Cont'd)

- Easy to use
- Hard to copy
- Easy to destroy

Quality Control

- Cycle random generator and test
- Testing for the failure of the generator, not for the quality of the method.

– Don't hash before testing.

Key Production Costs

- Physical
  - manufacturing rotors
  - permutor boards

Key Production Costs

- Logical
  - permutations for rotor wirings
  - primitive polynomials for shift registers
  - prime numbers for RSA keys

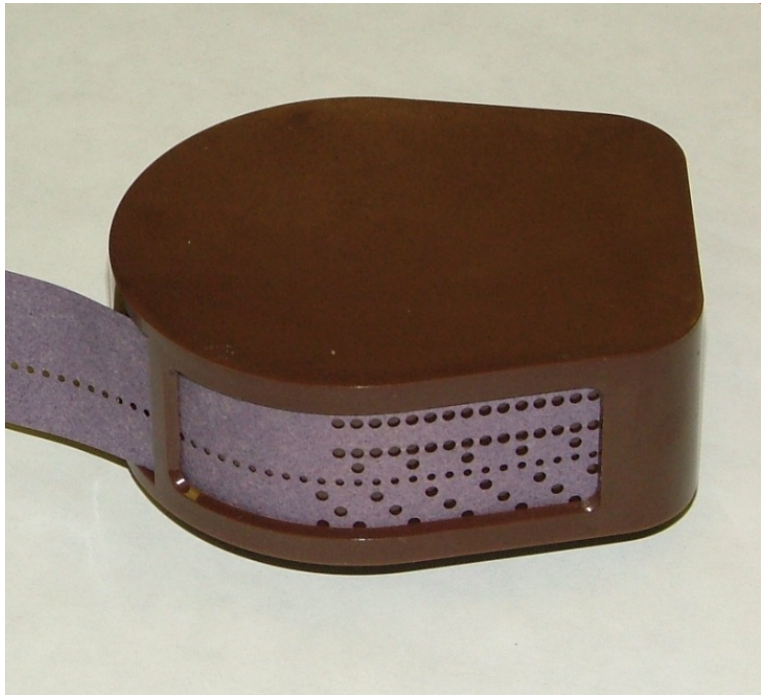
Distribution

- Shipping
- Encrypted transmission
- Quantum Key Distribution

Transport

- Paper tape in canisters
- KYK-13
- KSD64a (STU-III)
- Smart cards
- All ordinary data storage devices: CDCs, USBs, etc.

Key-tape Canister



Paper-tape Key Loader

KYK-13

KY-57


KY - 57
"VINSON"
Manpack Secure Voice
Half Duplex Wideband
Equipment shown here with PR -77 Radio
1970s - Present
TD
ON
OFF
VOLUME
AUDIO
FILL
MODE
PULL

Cable

Use

- Codebooks
- Rotor machine setup
- Plug boards
- Slide switches
- Pull paper tape, etc.

Accounting
(Comsec Materials Control System)

- Central Facility
- Comsec accounts
- Comsec Custodians and user agents
- Hand receipts
- Inventories

Destruction

- Lead jackets to sink codebooks
- Smashing rotors
- Burning or shredding cards and tapes

Destruction

- Zeroizing many forms of computer memory
- Physically destroying computer memory

Changing Keys

- Why change keys
  - Cryptoperiod (intrinsic)
  - Management issues (extrinsic)

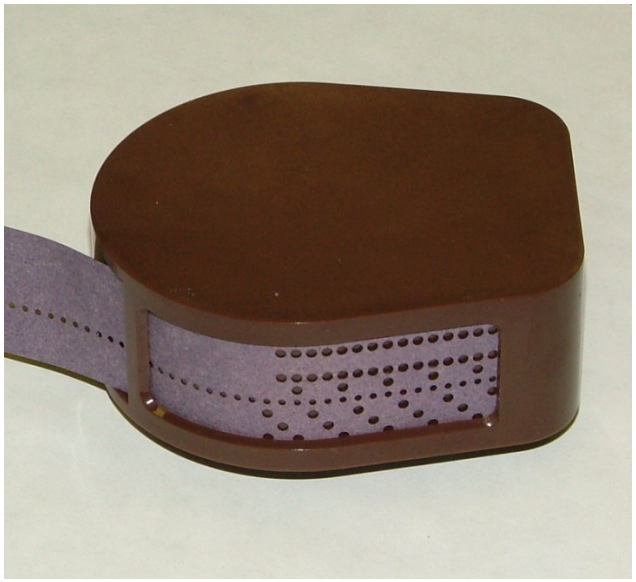
Changing Keys

- Rekeying
- Key Updating
  - backtrack security
- Daisy chaining (danger of cascading compromise)

Key Management Failures (Uninteresting)

- Boyce and Lee
- Helmich
- Walkers

Drove Transition from



To

Key Management Failure (Very Interesting)

- Venona
- Russian re-use of 1-time key
- Thirty-five year project.