Exploration of Cryptography

Whitfield Diffie

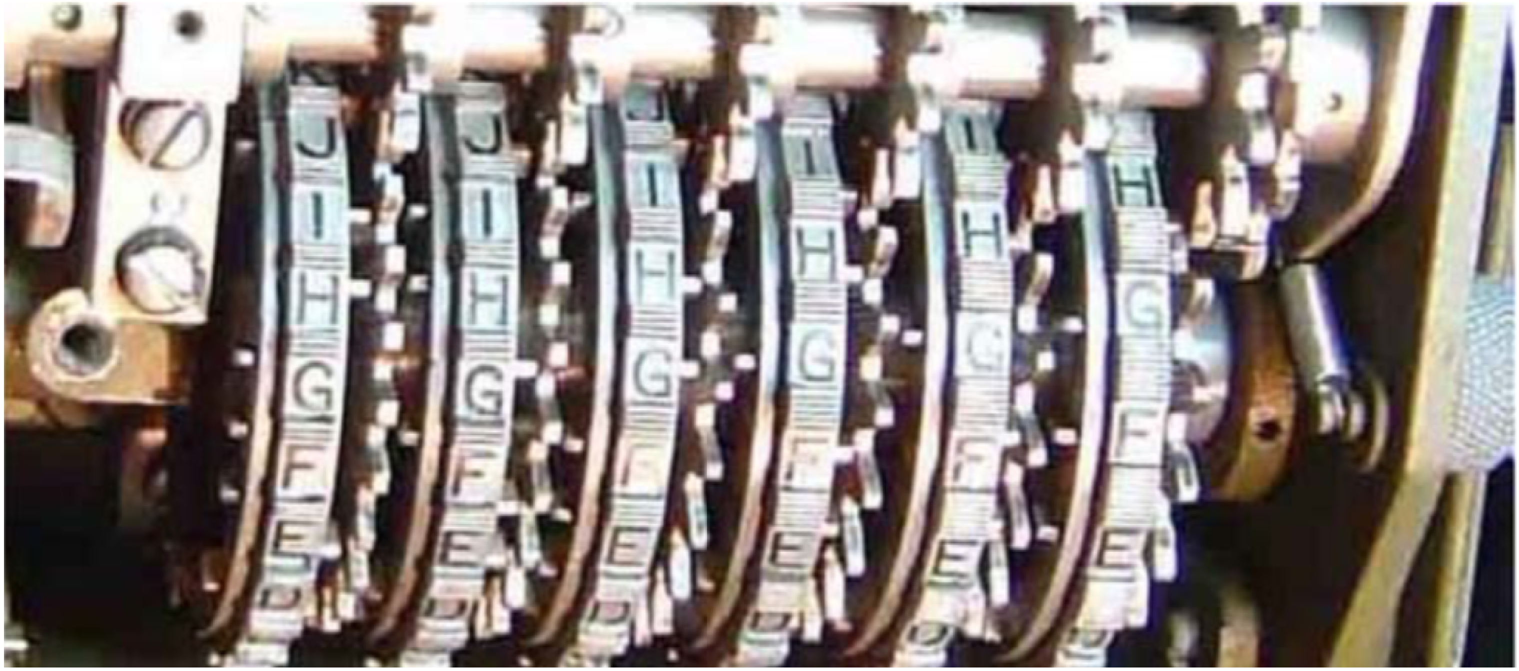
Distinguished Visiting Professor

Zhejiang University

Monday 14 December 2020

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:

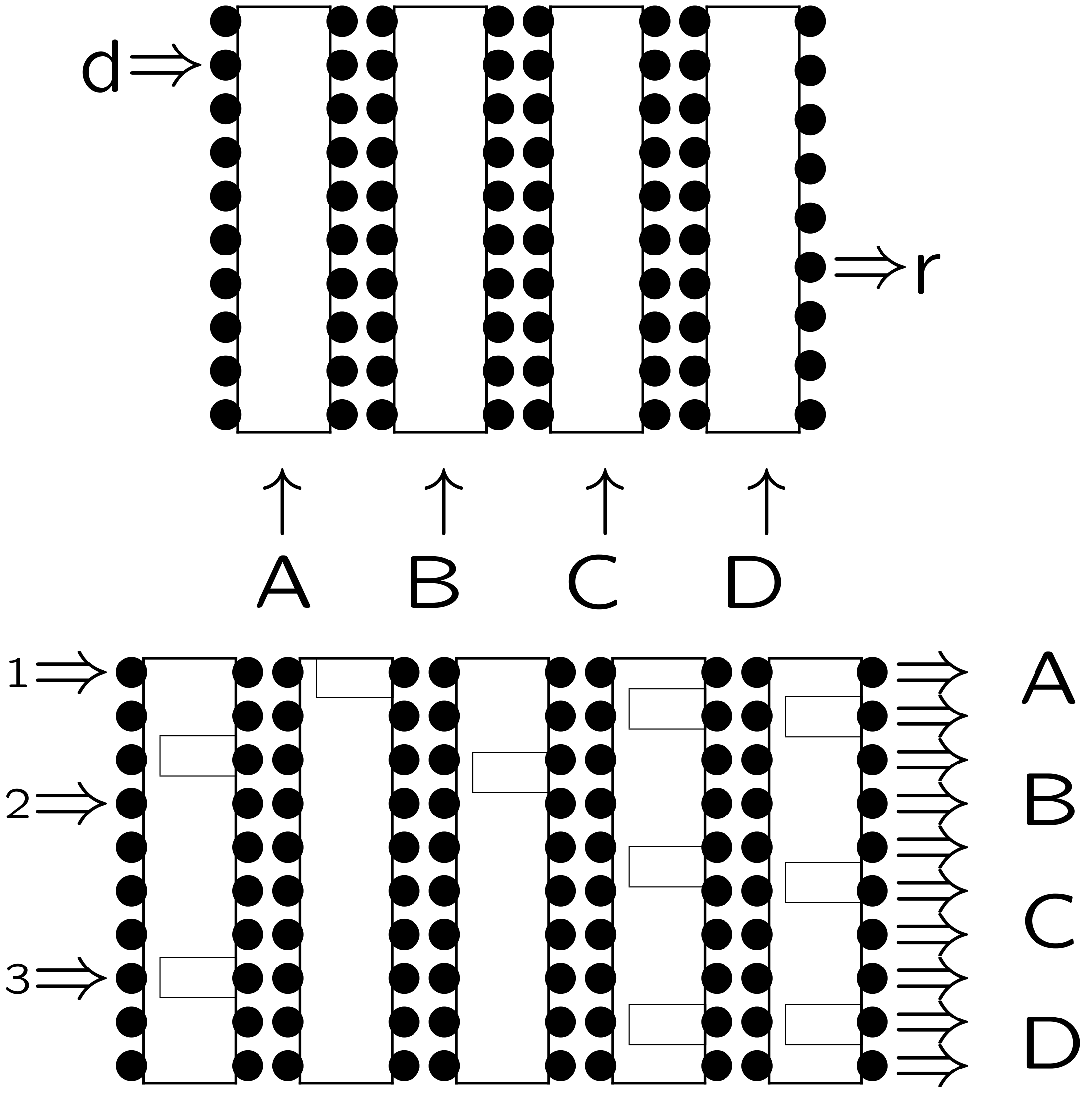
- 18: 1, 3, 5, 7, 9, 11, 13, 15, 17
- 17: 0, 1, 2, 3, 4, 5, 6, 7, 8
- 15: 7, 8, 9, 10, 11, 12, 13, 14
- 13: 2, 3, 4, 5, 6, 7, 8
- 11: 0, 2, 3, 5, 10

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?

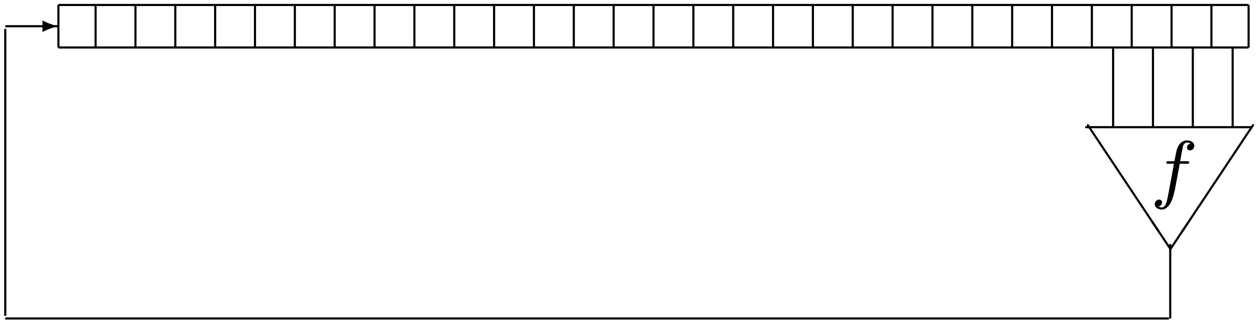
- What is the expected number of wheels that move at each clock tick?

4 - Sigbubba - bis

Since Sigbugga 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?