Exploration of Cryptography

Whitfield Diffie

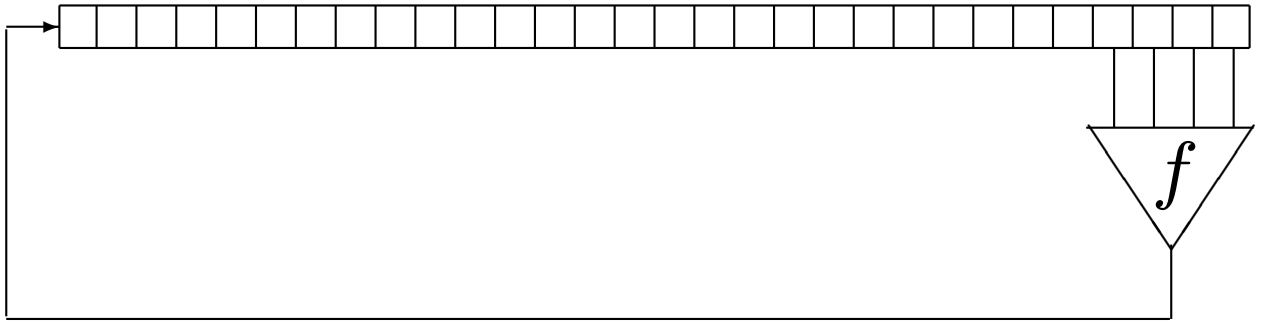
Distinguished Visiting Professor

Zhejiang University

Wednesday 8 April 2020

Homework

Nonlinear Feedback Shift Register



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

Cellular Automata in SM4

Two cellular automata are used in SM4, one in the encryption process and one in the key schedule. Determine whether these cellular automata are invertible.

Cellular Automata in SM4 (Cont'd)

You may either approach this problem theoretically or approach it experimentally by programming the automata and running them on the four-billion 32-bit words and testing for invertibility.

Variations on RSA

- Suppose that you were to consider employing the RSA cryptosystem with the modulus 35. What is wrong with that modulus other than the fact that it is much too small?

- Examine the smallest possible RSA moduli: $6 = 2 \times 3, 10 = 2 \times 5$, up through perhaps $143 = 11 \times 13, 323 = 17 \times 19$ or even $899 = 29 \times 31$. What is the smallest of these that exhibits the attractive properties of the RSA system, for example, keys should not be their own inverses. (In

class, I used $77 = 7 \times 11$. Is that a good tutorial choice? Can you find a better one?)