Data Encryption

- Abrie Greeff
- CS 778
- Project 6

Introduction

- Data security
- Public key vs private key
- Block cipher vs stream cipher

Constructing a cipher from a NFA

- Good transition rules

$$\delta(q_i, a) = \overline{\{q_i, q_{i+1}\}}, \; for \; 0 \le i \le n-2$$
$$\delta(q_{n-1}, a) = \overline{\{q_{n-1}\}}$$

Constructing a cipher from a NFA

- Transition table

δ	a
0	01
1	12
2	2

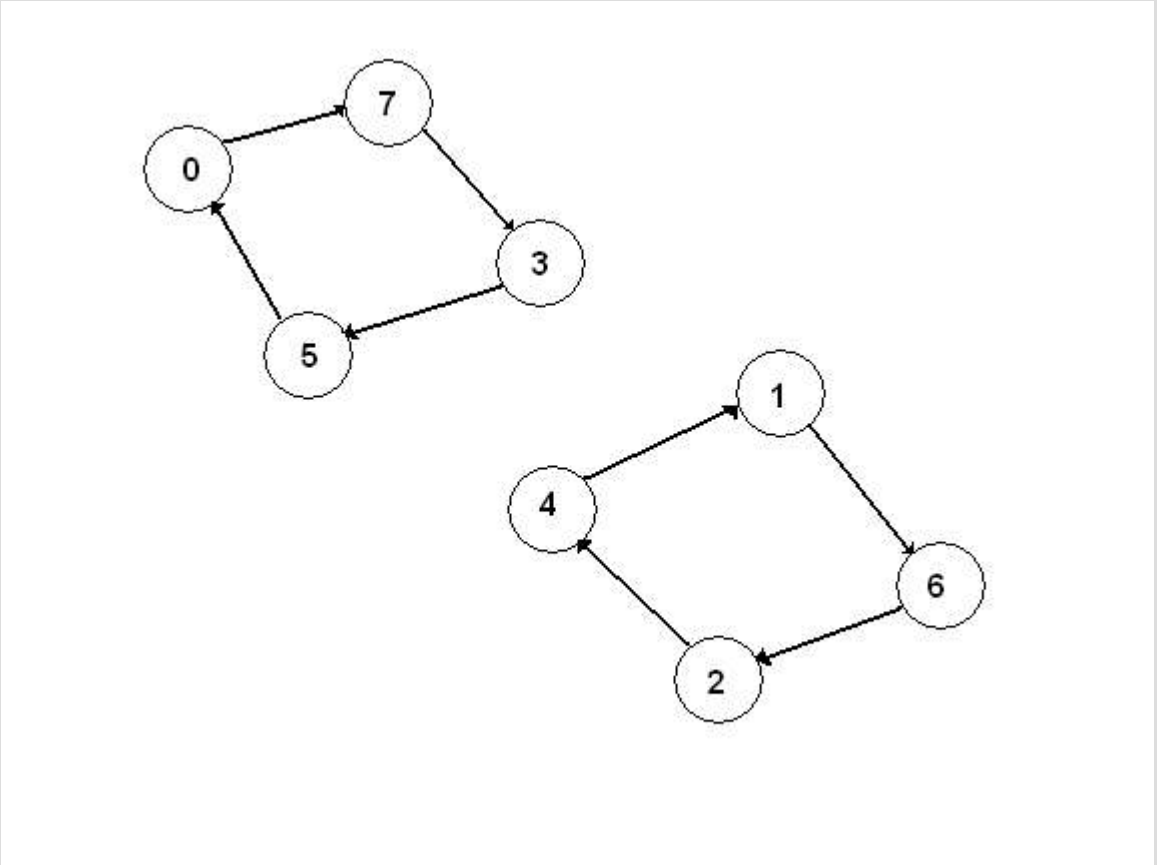
Constructing a cipher from a NFA

- Constructing the DFA
- XNOR operation

δ	a
0	7
1	6
2	4
3	5
4	1
5	0
6	2
7	3

Constructing a cipher from a NFA

- Cycles
- Encryption
- Decryption



Implementation

- Defining rules
- Storage of the DFA and NFA

Conclusion

- Permutation cipher
- Amount of bits
- Time complexity
- Breaking the encryption