CS3200: Computer Networks

Lecture 34

IIT Palakkad

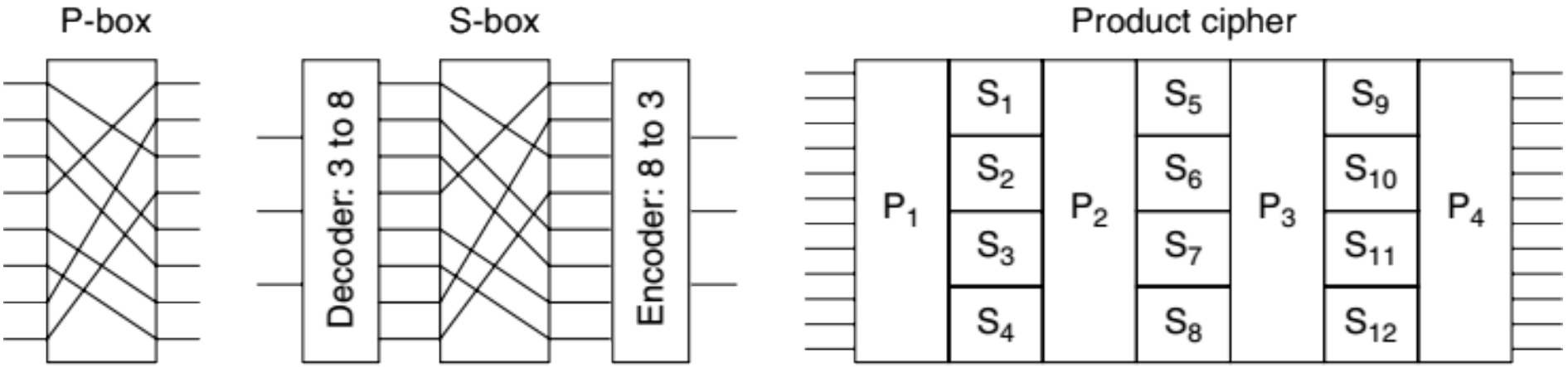
06 Nov, 2019

Symmetric-Key Algorithms

- Modern cryptography uses the same basic ideas as traditional cryptography (transposition and substitution).
- Make the encryption algorithm so complex and involuted that even if the cryptanalyst acquires vast mounds of enciphered text of his own choosing will not help.
- The first class of encryption algorithms we will study in this chapter are called **symmetric-key algorithms** because they use the same key for encryption and decryption.
- In particular, we will look at block ciphers, which take an n-bit block of plaintext as input and transform it using the key into an n-bit block of ciphertext.

P-box and S-box

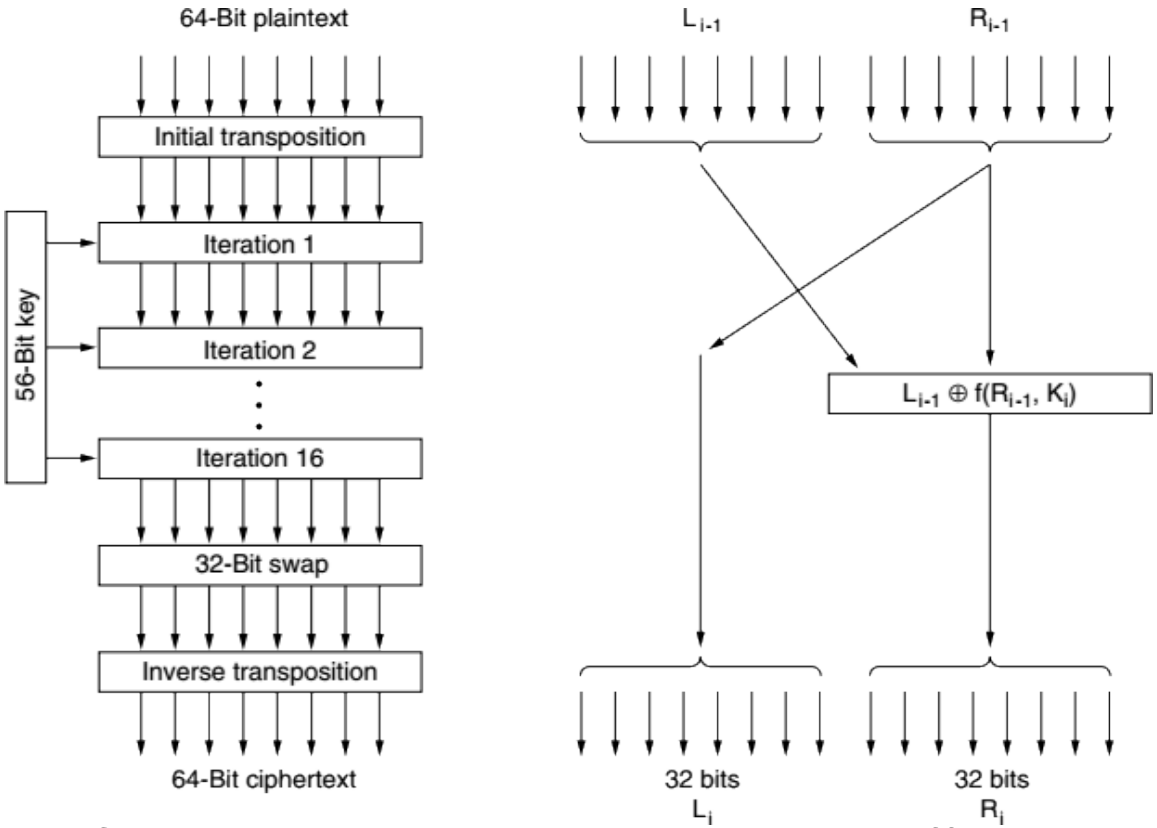
Transpositions and substitutions can be implemented with simple electrical circuits.



The real power of these basic elements only becomes apparent when we cas- cade a whole series of boxes to form a **product cipher**.

DES — The Data Encryption Standard

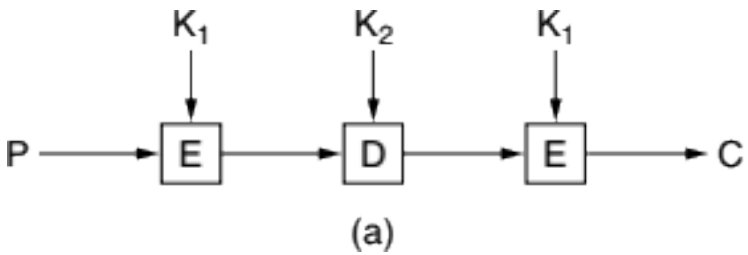
Is a 64-bit block cipher which was developed by IBM.

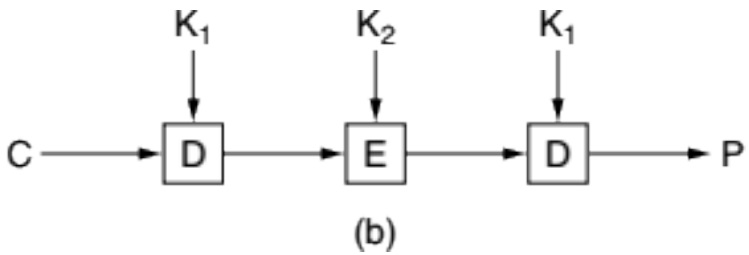


In 1977, two Stanford cryptography researchers, Diffie and Hellman (1977), designed a machine to break DES and estimated that it could be built for 20 million dollars. It is a reality now!!! and costs just $10,000.

Triple DES

Developed to overcome the flaws of DES. Uses to keys each of size 56-bits.





AES — The Advanced Encryption Standard

Read Section 8.2.2 of Tanenbaum.

Other Ciphers

Cipher	Author	Key length	Comments
DES	IBM	56 bits	Too weak to use now
RC4	Ronald Rivest	1–2048 bits	Caution: some keys are weak
RC5	Ronald Rivest	128–256 bits	Good, but patented
AES (Rijndael)	Daemen and Rijmen	128–256 bits	Best choice
Serpent	Anderson, Biham, Knudsen	128–256 bits	Very strong
Triple DES	IBM	168 bits	Good, but getting old
Twofish	Bruce Schneier	128–256 bits	Very strong; widely used

Cryptanalysis

- **Differential cryptanalysis** can be used to attack any block cipher. It works by beginning with a pair of plaintext blocks differing in only a small number of bits and watching carefully the cipher text.
- **Linear cryptanalysis** (Matsui, 1994) can break DES with only 2^{43} known plaintexts. It works by XORing certain bits in the plaintext and ciphertext together and examining the result.
- **Power analysis**: Processing a 1 takes more electrical energy than processing a 0. From this data, deducing the key is surprisingly easy. This kind of cryptanalysis can be defeated only by carefully coding the algorithm in assembly language to make sure power consumption is independent of the key and also independent of all the individual round keys.