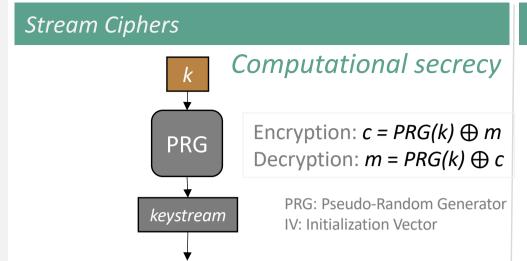
Pages on SecuRity by Ruxandra F. Olimid

16



1 bit

• encrypts bit-by-bit

1 bit

 the encryption of one bit is independent on the value of other bits in the plaintext (but only depends on the corresponding bit)

Less resources



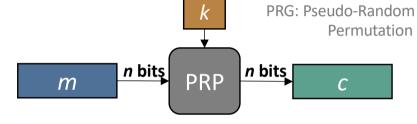
Many broken



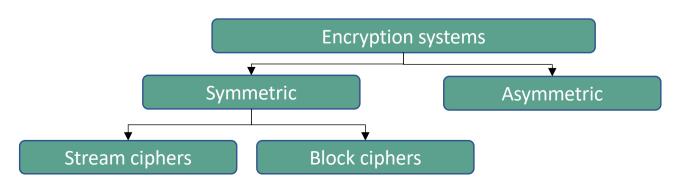
Block Ciphers

Computational secrecy

Encryption: c = PRP(k,m)Decryption: $m = PRP^{-1}(k,c)$



- encrypts in blocks of bits
- the encryption is dependent on the values of all bits in plaintext block
- More resources
- Seem more secure



draolimid.weebly.com/pagesonse