SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

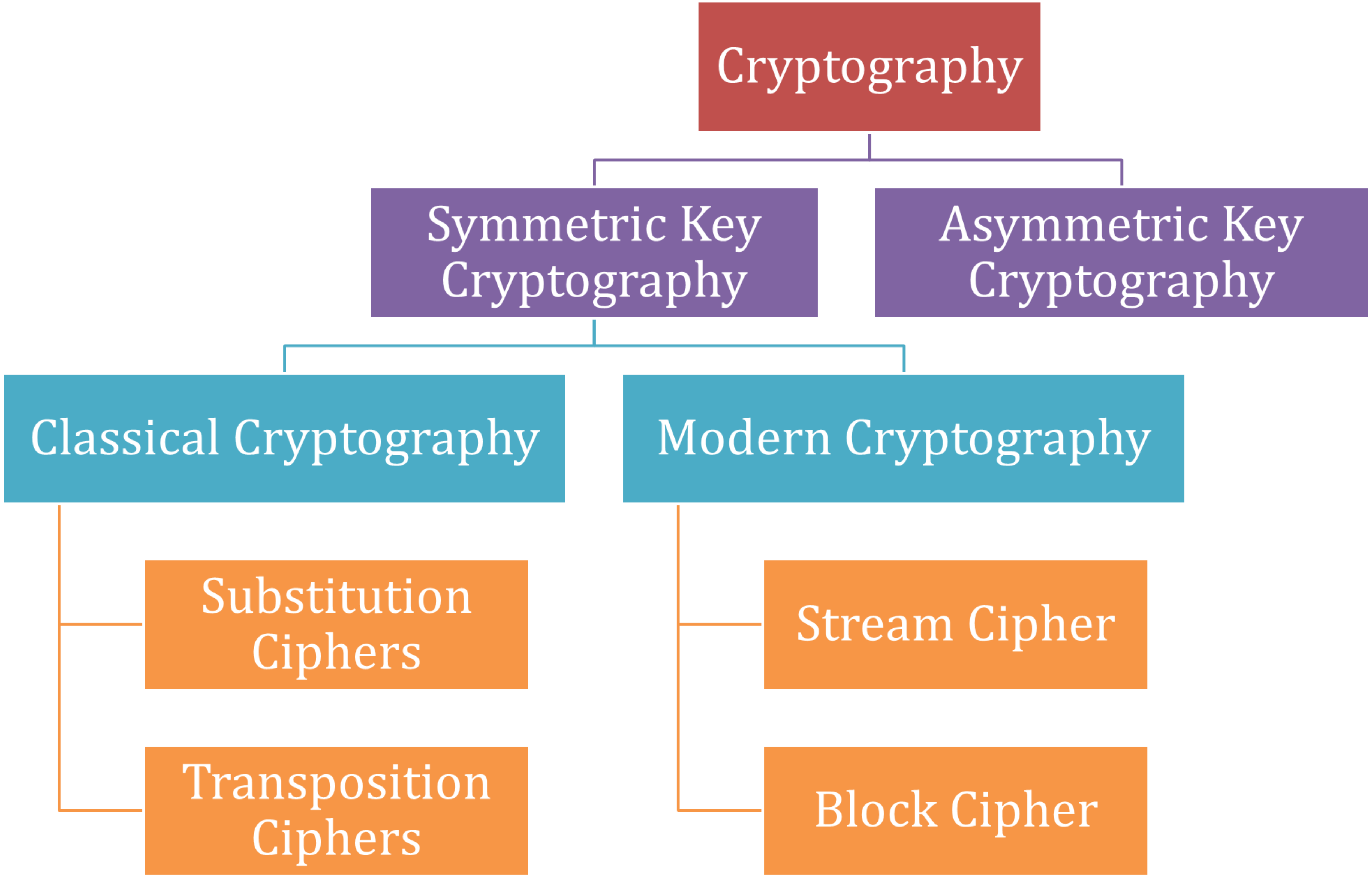
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

COURSE NAME : 19CS503 Cryptography and Network Security

III YEAR /V SEMESTER

Unit 1- Introduction

Topic : Foundations of modern cryptography



Cryptography

Symmetric Key Cryptography

Asymmetric Key Cryptography

Classical Cryptography

Modern Cryptography

Substitution Ciphers

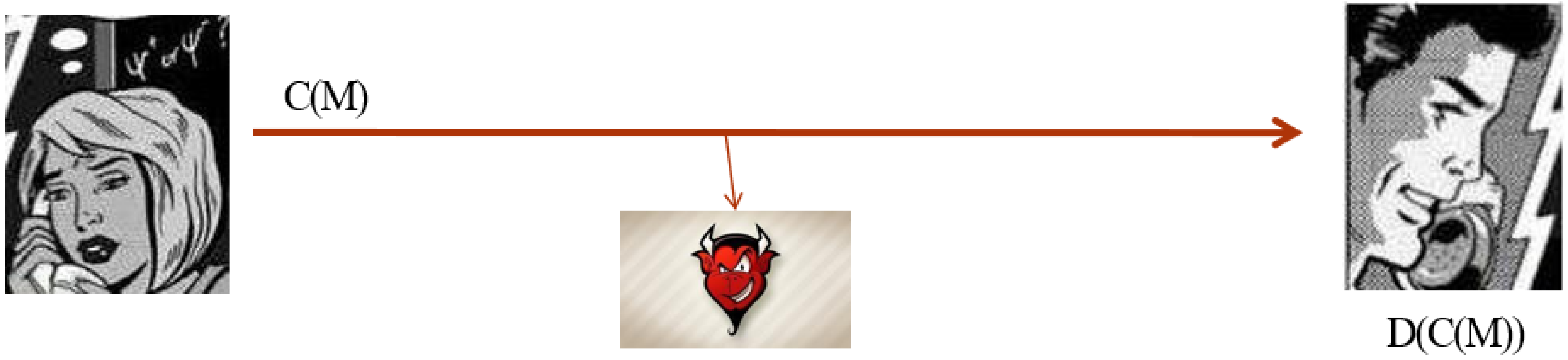
Transposition Ciphers

Stream Cipher

Block Cipher

Modern Cryptography

- *Cryptography*:The art of writing or solving codes.
- Classical cryptography: The art of secret writing.



- The communication is secure as long as the encoding algorithm is a *secret*.
  - Disadvantages: Reverse engineering, coding algorithm leaks.

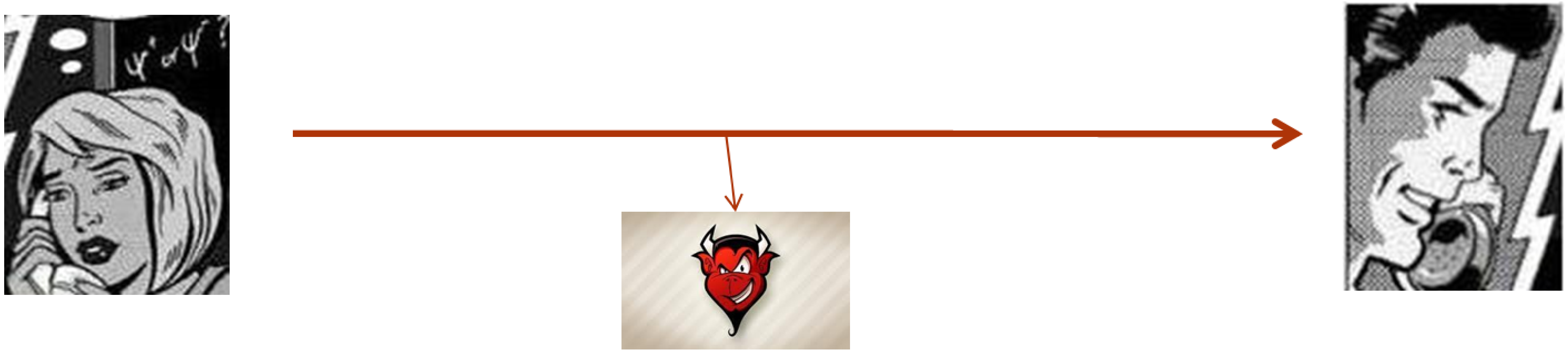
Modern Cryptography

- Cryptography: The scientific study of techniques for securing digital information, transaction, and distributed computations.
- Classical cryptography was restricted to military. Modern cryptography is influences almost everyone.
- Classical cryptography was mostly about secret communication. With modern cryptography the scope has expanded. It now deals with digital signatures, digital cash, secure voting…
- Modern cryptography breaks out of the “design-break-design” cycle model of classical cryptography.
- The security is not based on the secrecy of the protocol details but based on sound mathematical and computational principles.
- Provable security: It is now possible to formally argue about the security of protocols.

Foundations of Modern Cryptography

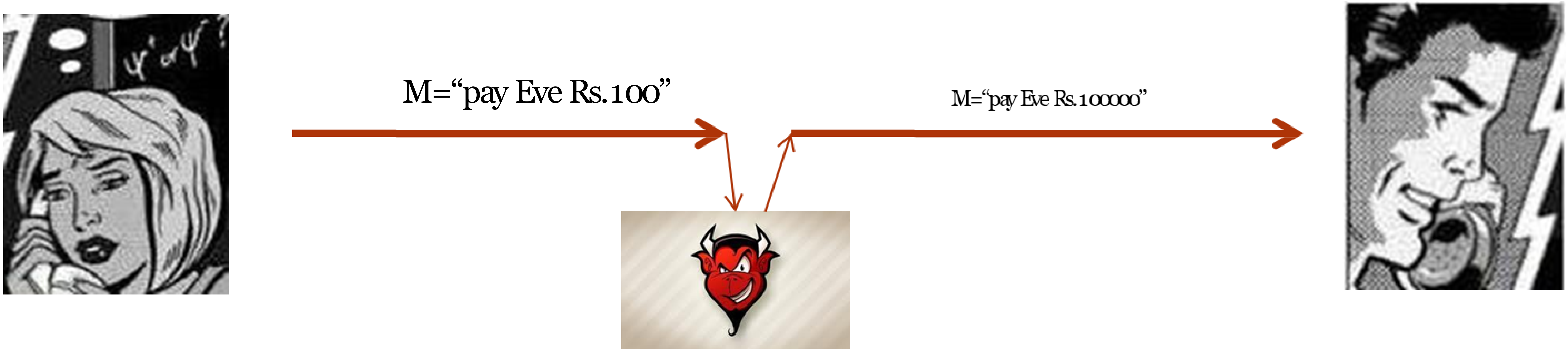
Privacy

- □ Alice wants to send a message to Bob without an adversary Eve figuring out the message.



Integrity and Authenticity

- □ Bob wants to make sure that the message that he received from Alice is indeed sent by her and not modified during transit.



M="pay Eve Rs.100"

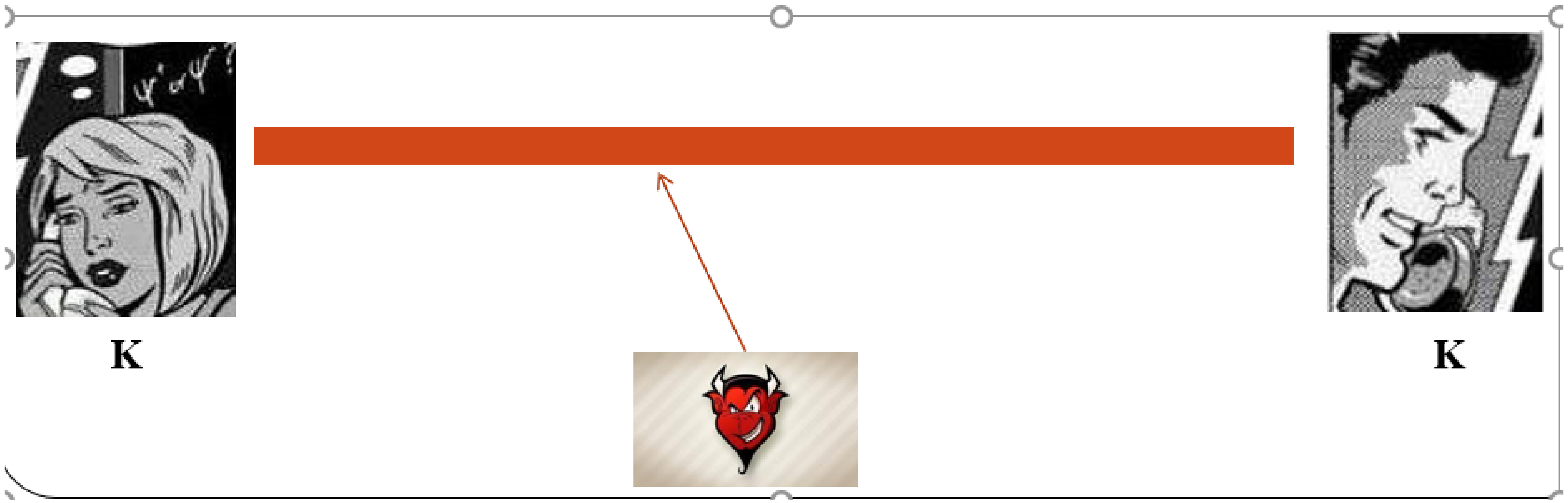
M="pay Eve Rs.100000"

Perfect world

- There is a super-strong pipe between Alice and Bob.
- Both privacy and authenticity goals are met.

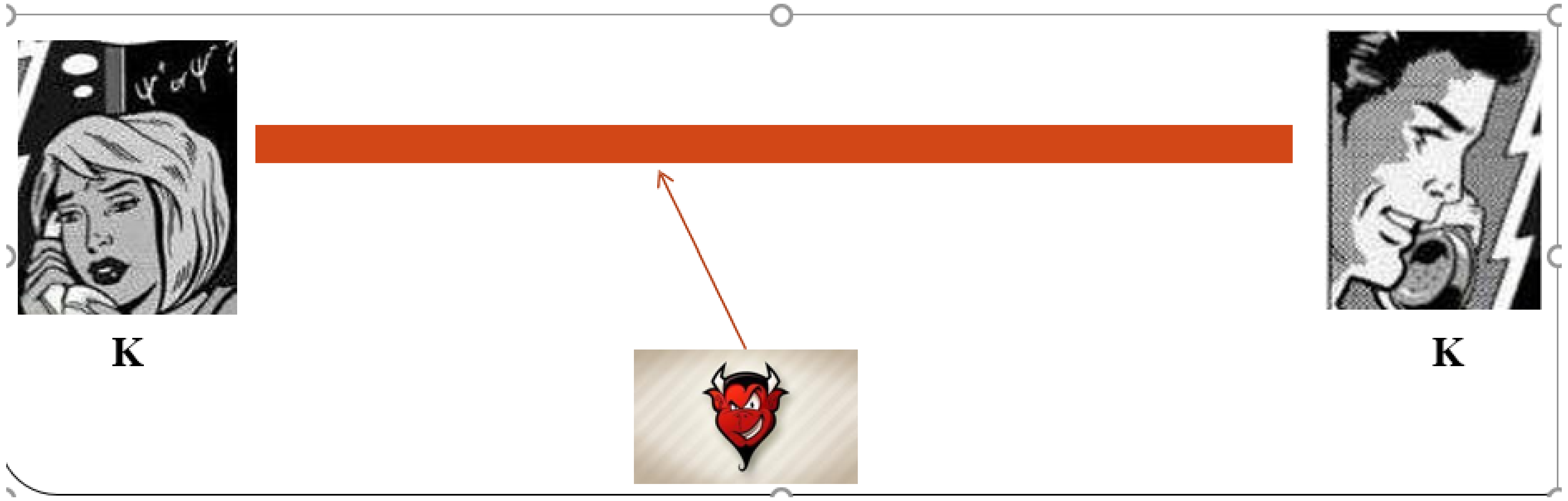
Real world

- The channel between Alice and Bob is public.
- Assume that Alice and Bob share some secret K.
- Alice encodes her message M using a public encryption algorithm E and K.We write C = EK(M).
- Bob decrypts Alice’s message using a public decryption
- algorithm D and K. We write M = DK(C).



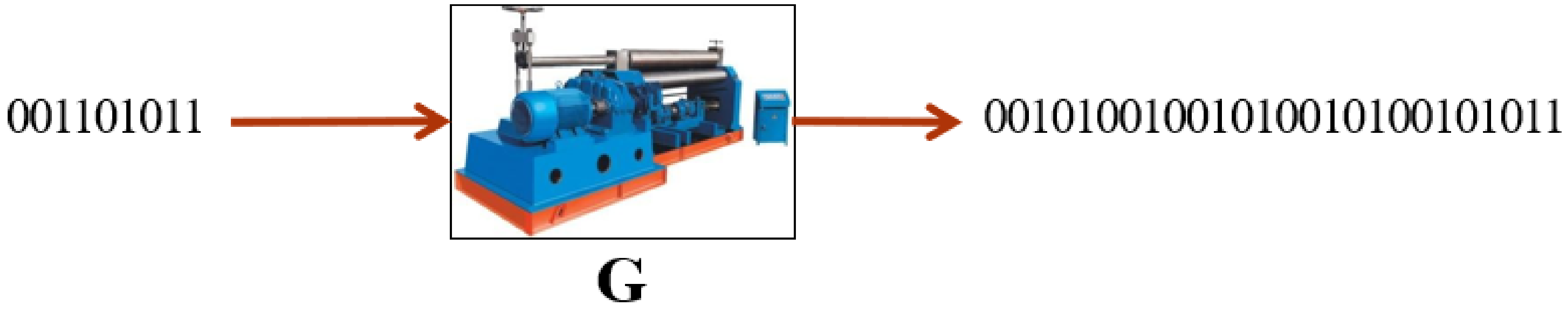
Shannon’s one time pad

- EK(M) = K (XOR) M
- Example:
- 101 (XOR) 111 = 010
- 101 (XOR) 010 = 111
- Is this protocol secure?
- Yes.The adversary can only guess each bit with probability ½.
- Problem:The key is as long as the message.



Pseudo randomness

- Suppose there was a *generator* that *stretches* random bits.



001101011

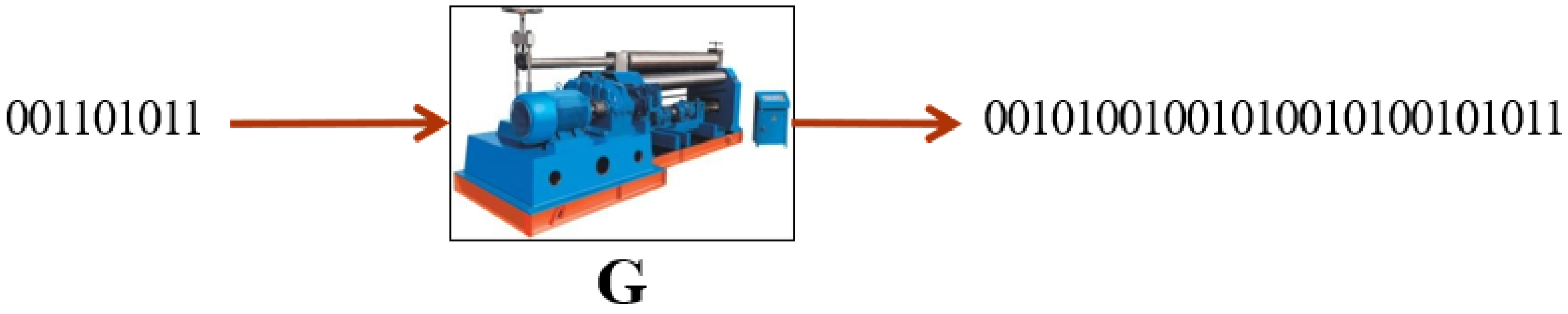
00101001001010010100101011

G

- Idea:
  - Choose a short key **K** randomly.
  - Obtain **K'=G(K)**.
  - Use **K'** as key for the one time pad.
- Issue: ?

Pseudo randomness

- Suppose there was a *generator* that *stretches* random bits.



001101011

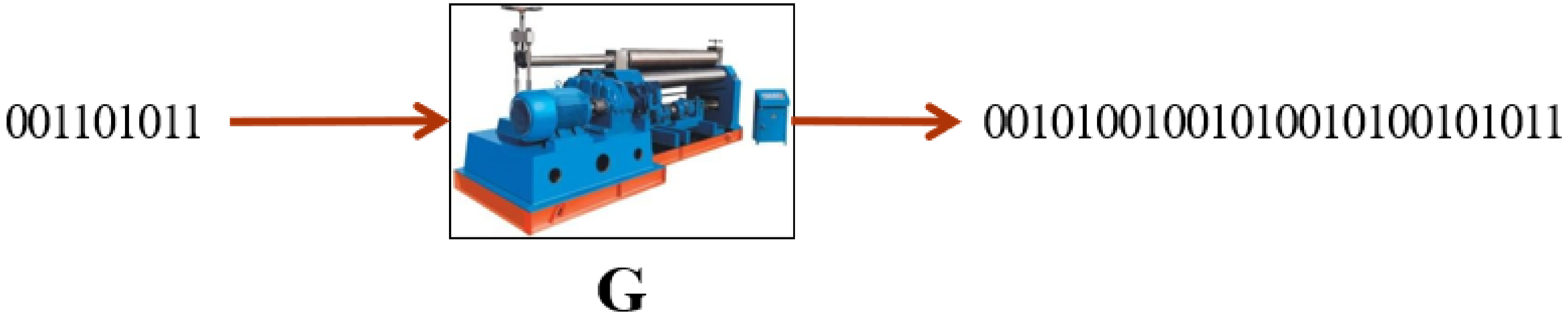
00101001001010010100101011

G

- Idea:
  - Choose a short key **K** randomly.
  - Obtain **K’=G(K)**.
  - Use **K’** as key for the one time pad.
- Issue:
  - Such a generator is not possible!
  - Any such generator produces a longer string but the string is not *random*.

Pseudo randomness

- Suppose there was a *generator* that *stretches* random bits.

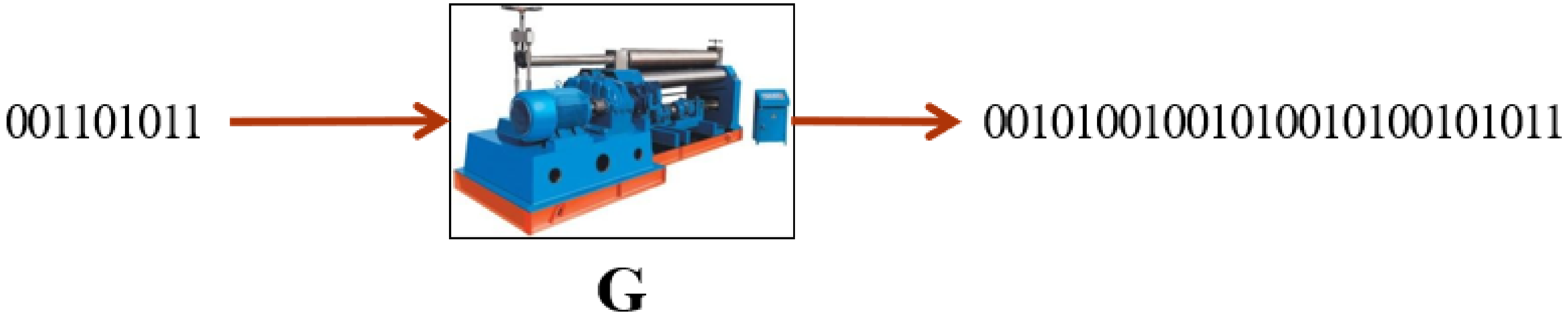


001101011 → G → 00101001001010010100101011

- Approach for proving security:
  - Carefully define pseudorandomness (“appears to be random”).
  - Argue that if there is an adversary that *breaks* the protocol (our one time pad), then the bit string produced by **G** is not really pseudorandom.

Pseudo randomness

- Suppose there was a *generator* that *stretches* random bits.



001101011

0010100100101001010010100101011

G

- Approach for proving security:
  - Carefully define pseudorandomness (“appears to be random”).
  - Argue that if there is an adversary that *breaks* the protocol (our one time pad), then the bit string produced by **G** is not really pseudorandom.

CRYPTANALYSIS

Cryptanalysis

□ Cryptanalysis is the decryption and analysis of codes, ciphers or encrypted text. Cryptanalysis uses mathematical formulas to search for algorithm vulnerabilities and break into cryptography or information security systems

Cryptanalysis

- Practice of analyzing and breaking cryptography
- Resistance to crypt analysis is directly proportional to the key size
- With each extra byte strength of key doubles
- Cracking Pseudo Random Number Generators
- A lot of the encryption algorithms use PRNGs to generate keys which can also be cracked leading to cracking of algorithms
- Variety of methods for safe guarding keys (Key Management)
- Encryption & computer access protection
- Smart Cards

Cryptanalysis attack

- □ Known-Plaintext Analysis (KPA): Attacker decrypt ciphertexts with known partial plaintext.
- □ Chosen-Plaintext Analysis (CPA): Attacker uses ciphertext that matches arbitrarily selected plaintext via the same algorithm technique.
- □ Ciphertext-Only Analysis (COA): Attacker uses known ciphertext collections.
- □ Man-in-the-Middle (MITM) Attack: Attack occurs when two parties use message or key sharing for communication via a channel that appears secure but is actually compromised. Attacker employs this attack for the interception of messages that pass through the communications channel. Hash functions prevent MITM attacks.
- □ Adaptive Chosen-Plaintext Attack (ACPA): Similar to a CPA, this attack uses chosen plaintext and ciphertext based on data learned from past encryptions.

Assessment

Compute the Ciphertext using Playfair Cipher

Perform Encryption and decryption using Playfair cipher for the following Message **hi where are you** and Key: **monarchy**

REFERENCES

1. William Stallings, Cryptography and Network Security, 6 th Edition, Pearson Education, March 2013.

THANK YOU