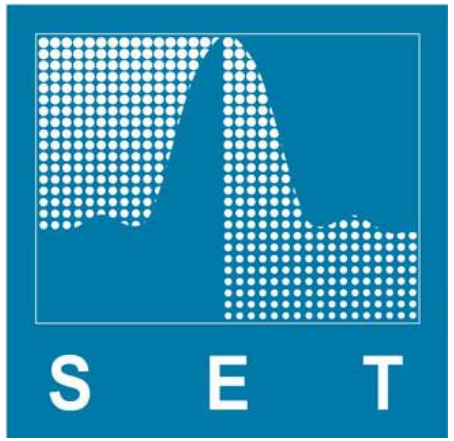


Hanoi University of Science and Technology

School of Electronics and Telecommunications

CRYPTOGRAPHY THEORY

Lecturer : Assoc. Prof. Do Trong Tuan

Group : 01

Members of group:

1. *Luong Van Minh*
2. *Hoang Tuan Anh*
3. *Tran Manh Cuong*
4. *Nguyen Anh Dung*
5. *Do Thi Thuy Kieu*

Topic Hash Function

SHA-512

Plan of “campaign”

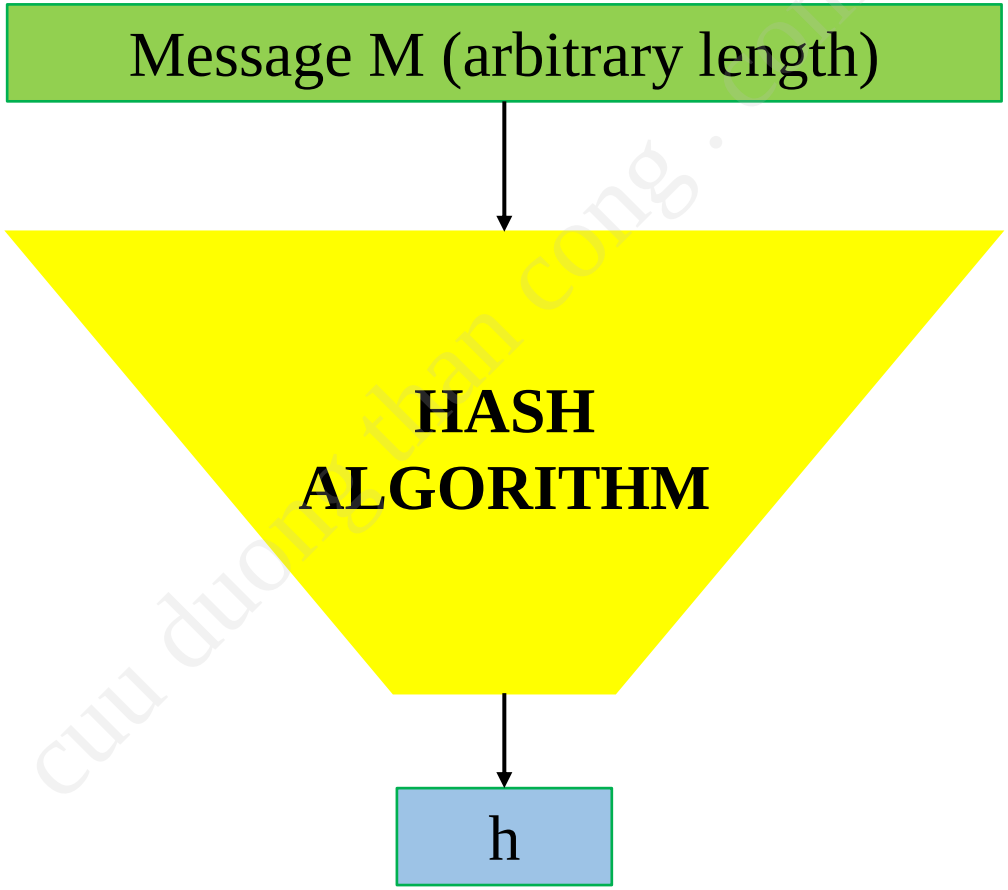
1. Hash Function

2. SHA

3. SHA-512

4. Implement program by C language

Hash Function



Hash value (fixed length)

Application

- Check the security of transmission channel
- Check the integrity of the data

SHA (Secure Hash Algorithm)

SHA is the algorithms used to convert a certain piece of data into a fixed length piece of data with high probability of difference.

- *It is computationally infeasible to find a message that corresponds to a given message digest*
- *It is computationally infeasible to find 2 different messages that produce the same message digest*
- *Any change to the message will make a absolutely different message digest with a very high probability*

SHA Algorithms

- SHA-1 → *Not secure*
- SHA-224
- SHA-256
- SHA-384
- SHA-512

SHA-512

- SHA-512 is a Hash Algorithm
- Message length < 2^{128} bit
- Compression function operates on a block of 1024 bits and a hash value of 512 bits
- It’s mainly a block-cipher algorithm

Thank you for your listening