“बेटी बचाओ, बेटी पढ़ाओ”

JAYOTI VIDYAPEETH WOMEN'S UNIVERSITY, JAIPUR
Government of Rajasthan established
Through ACT No. 17 of 2008 as per UGC ACT 1956
NAAC Accredited University

Faculty of Education and methodology

Department of Science and Technology

Faculty Name- Jv’n Narendra Kumar Chahar (Assistant Professor)

Program- B.Tech 8thSemester

Course Name– Cryptography and Network Security

Session no.: 25

Session Name-Authentication Functions

Academic Day starts with –

- Greeting with saying **‘Namaste’** by joining Hands together following by 2-3 Minutes Happy session, Celebrating birthday of any student of respective class and **National Anthem.**

Lecture starts with- quotations’ answer writing

Review of previous Session **– Authentication Requirements**

Topic to be discussed today- Today We will discuss about **Authentication Functions**

Lesson deliverance (ICT, Diagrams & Live Example)-

- ➢ Diagrams

Introduction & Brief Discussion about the Topic**– Authentication Functions**

Authentication Functions

Any message authentication or digital signature mechanism can be viewed as having fundamentally two levels. At the lower level, there may be some sort of function that produces an authenticator: a value to be used to authenticate a message. This lower layer function is then used as primitive in a higher-layer authentication protocol that enables a receiver to verify the authenticity of a message.

The different types of functions that may be used to produce an **authenticator**

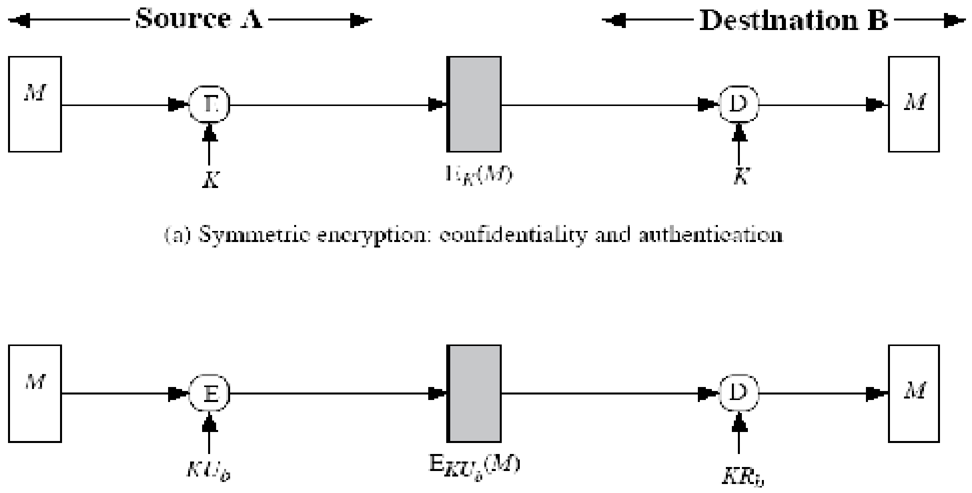
are as follows:

1. **Message encryption** – the cipher text of the entire message serves as its authenticator.
2. **Message authentication code (MAC)** – a public function of the message and a secret key that produces a fixed length value serves as the authenticator.

3. **Hash function** – a public function that maps a message of any length into a fixed length hash value, which serves as the authenticator.

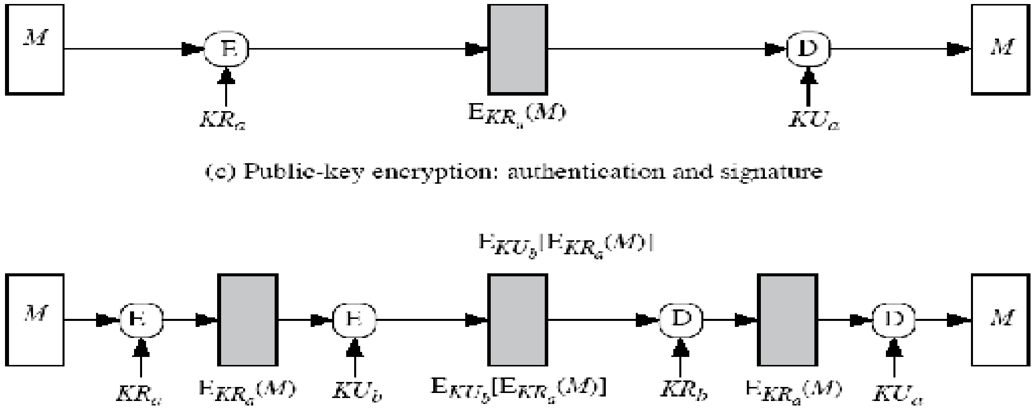
Message encryption

Message encryption by itself can provide a measure of authentication. The analysis differs from symmetric and public key encryption schemes.



(a) Symmetric encryption: confidentiality and authentication

(b) Public key encryption: confidentiality



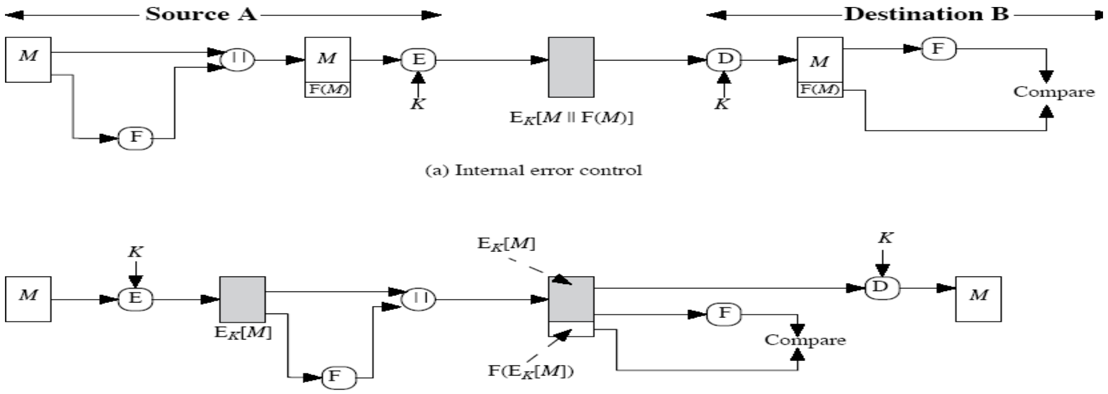
(c) Public-key encryption: authentication and signature

(d) Public-key encryption: confidentiality, authentication, and signature

Suppose the message can be any arbitrary bit pattern. In that case, there is no way to determine automatically, at the destination whether an incoming message is the ciphertext of a legitimate message. One solution to this problem is to force the plaintext to have some structure that is easily recognized but that cannot be replicated without recourse to the encryption function. We could, for example, append an error detecting code, also known as Frame Check Sequence (FCS) or checksum to each message before encryption

‘A’ prepares a plaintext message M and then provides this as input to a function F that produces an FCS. The FCS is appended to M and the entire block is then encrypted. At the destination, B decrypts the incoming block and treats the result as a message with an appended FC. B applies the same function F to attempt to reproduce the FCS. If the calculated FCS is equal to the incoming FCS, then the message is considered authentic.

In the internal error control, the function F is applied to the plaintext, whereas in external error control, F is applied to the ciphertext (encrypted message).



(a) Internal error control

(b) External error control

Reference-

1. **Book:** William Stallings, “Cryptography & Network Security”, Pearson Education, 4th Edition 2006.

QUESTIONS: -

Q1. What are the authentication functions in cryptography?

Q2. What are the different types of functions in authentication functions?

Next, we will discuss more about Message Authentication Code (MAC).

.

- Academic Day ends with-
  National song ‘Vande Mataram’