Computer Network Security

TE - IT

Lecture -13
09/08/2022

Session: 12:00 - 1:00 PM

Prof. Stella J
Department of Information Technology
Xavier Institute of Engineering

Module-2

Message Authentication Codes

- ✓ HMAC
- ✓ CMAC

Digital Signature

- ✓ RSA Approach
- ✓ DSA / DSS Approach

Message Authentication Code

Message Authentication Code (MAC), also referred to as a tag, is used to **authenticate the origin and nature of a message**. MACs use authentication cryptography to verify the legitimacy of data sent through a network or transferred from one person to another.

In other words, MAC ensures that the message is coming from the correct sender, has not been changed, and that the data transferred over a network or stored in or outside a system is legitimate and does not contain harmful code. MACs can be stored on a hardware security module, a device used to manage sensitive digital keys.

Message Authentication Code Steps:

1. MAC process is the **establishment of a secure channel** between the receiver and the sender.
2. To **encrypt a message**, the MAC system uses an algorithm, which uses a symmetric key and the plain text message being sent.
3. The MAC algorithm then **generates authentication tags** of a fixed length by processing the message.
4. The resulting computation is the message's MAC.
5. This **MAC is then appended** to the message and transmitted to the receiver.
6. The receiver **computes the MAC using the same algorithm.**
7. If the resulting MAC the receiver arrives at equals the one sent by the sender, the message is verified as authentic, legitimate, and not tampered with.

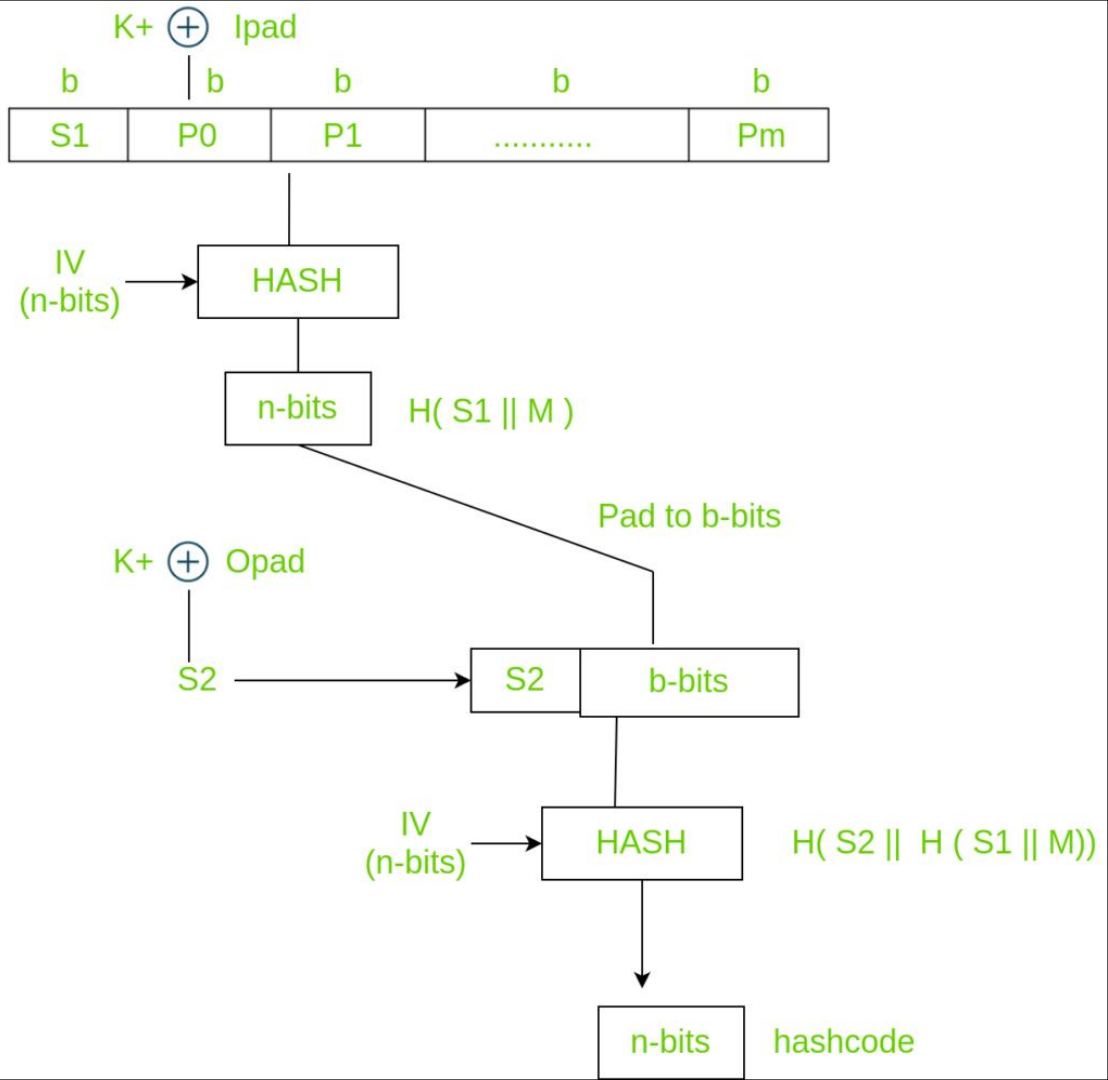
HMAC:

1. Select key (0<k<b)
b = b bits, key should be in the range of b bits

if k<b pad 0's on the left side until k=b

2. S1 = XOR K^+ with ipad
where, ipad = 00110110

3. Append S1 with message
4. Apply SHA-1/SHA-256/SHA-512 on the (S1||M)
5. Pad n bits until length equal to b bits.
6. S2 = XOR K^+ with Opad
where, opad = 01011100
7. Append S2 with o/p of Step6
8. Apply SHA Algorithm to get final Hash code



CMAC:

CO = E(A0, K0)
C1 = E(K1, A1 XOR C0)
C2 = E(K2, A2 XOR C1)

CN= E(Kn, An XOR Cn-1)

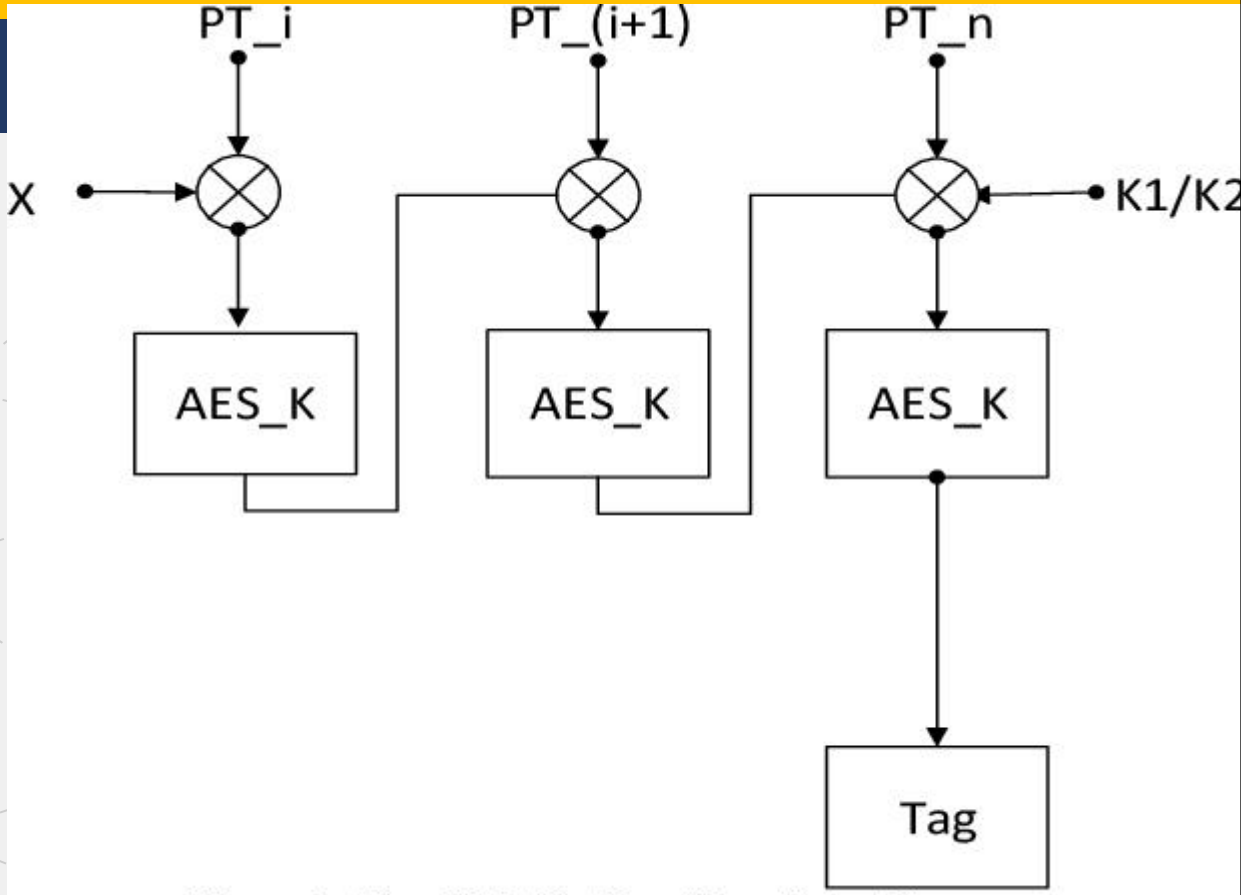
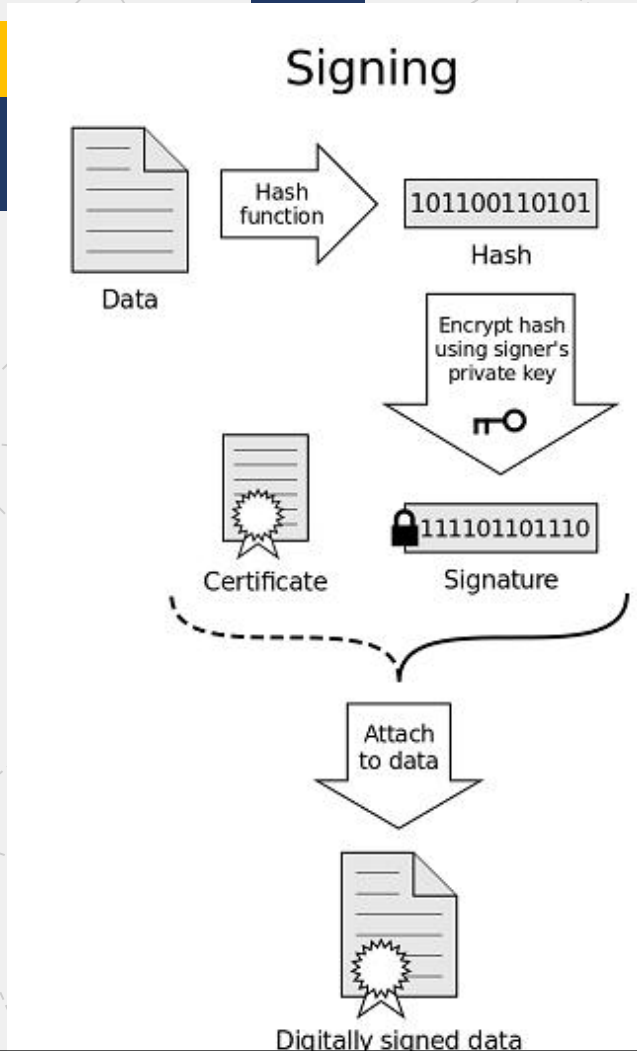


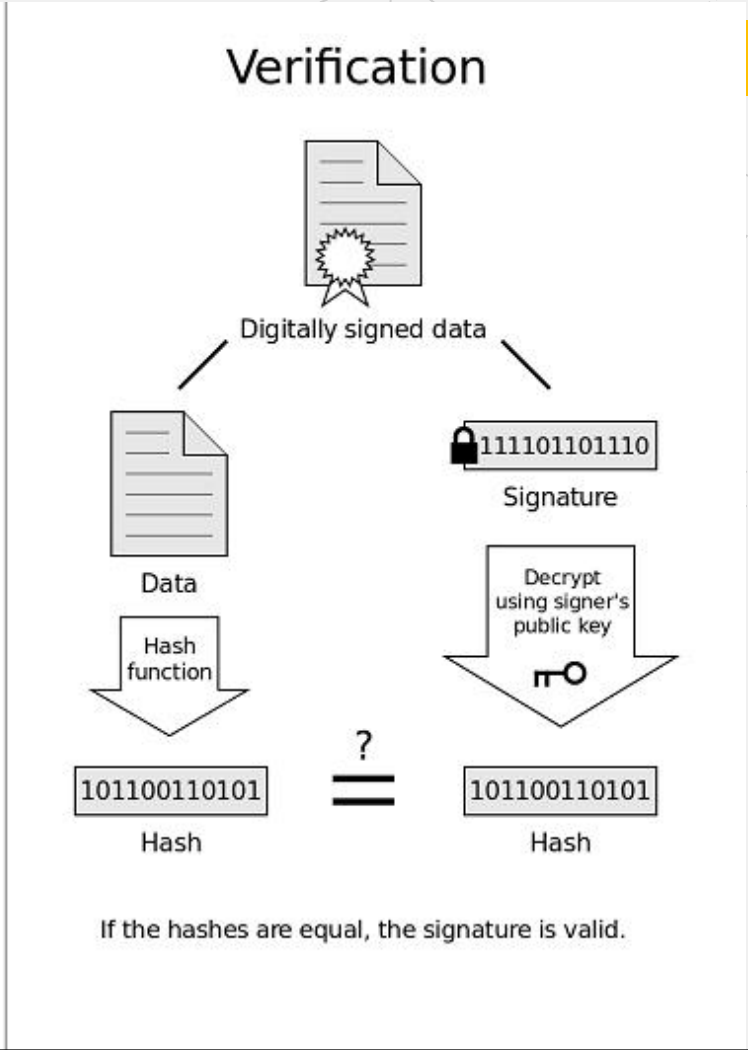
Figure 1. The CMAC Algorithm Flow Diagram

Digital Signature:

A Digital Signature is, in reality, nothing more than a numeric string that can be affixed to emails, documents, certificates almost anything. We use digital signatures to help determine authenticity and to validate identity. It’s not the same as encryption, it actually works in conjunction with encryption. Digital Signatures fall more into the category of hashing.

Digital Signature

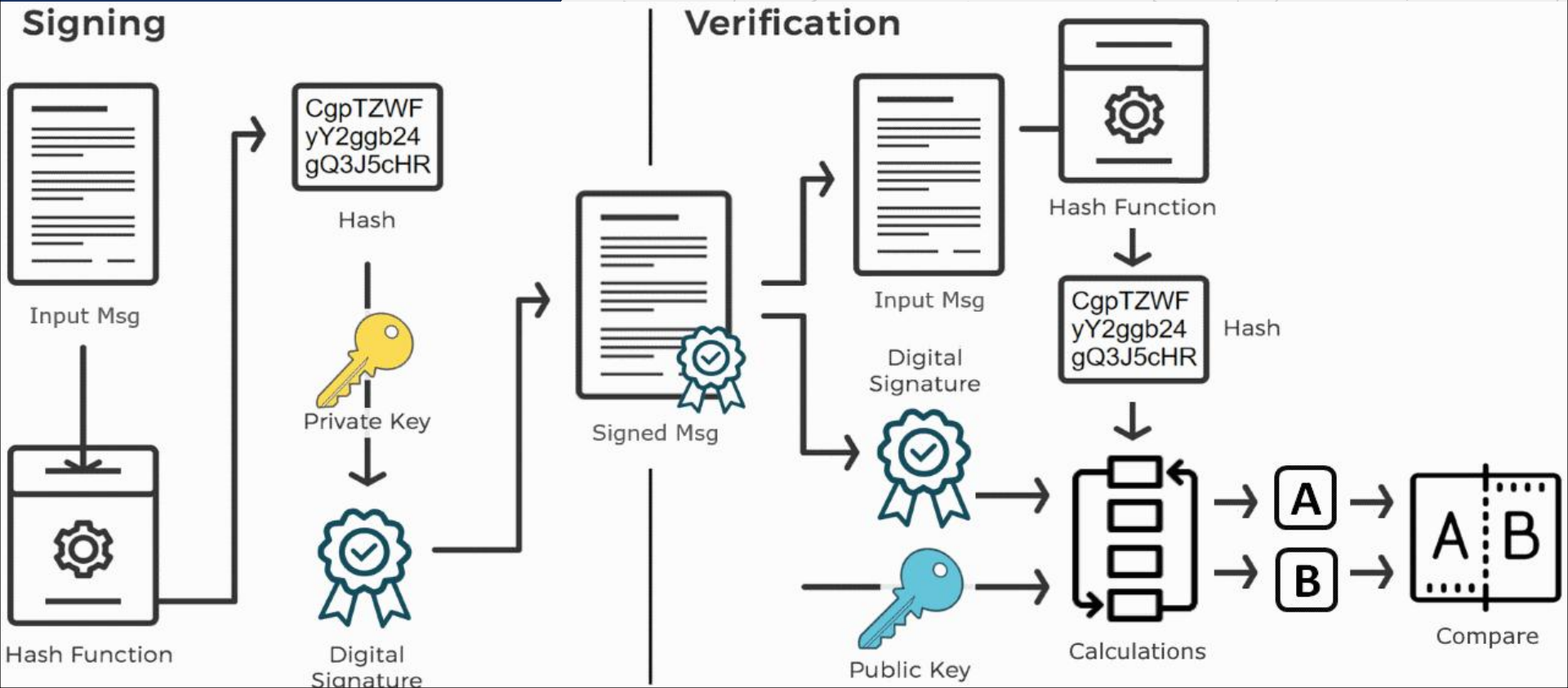




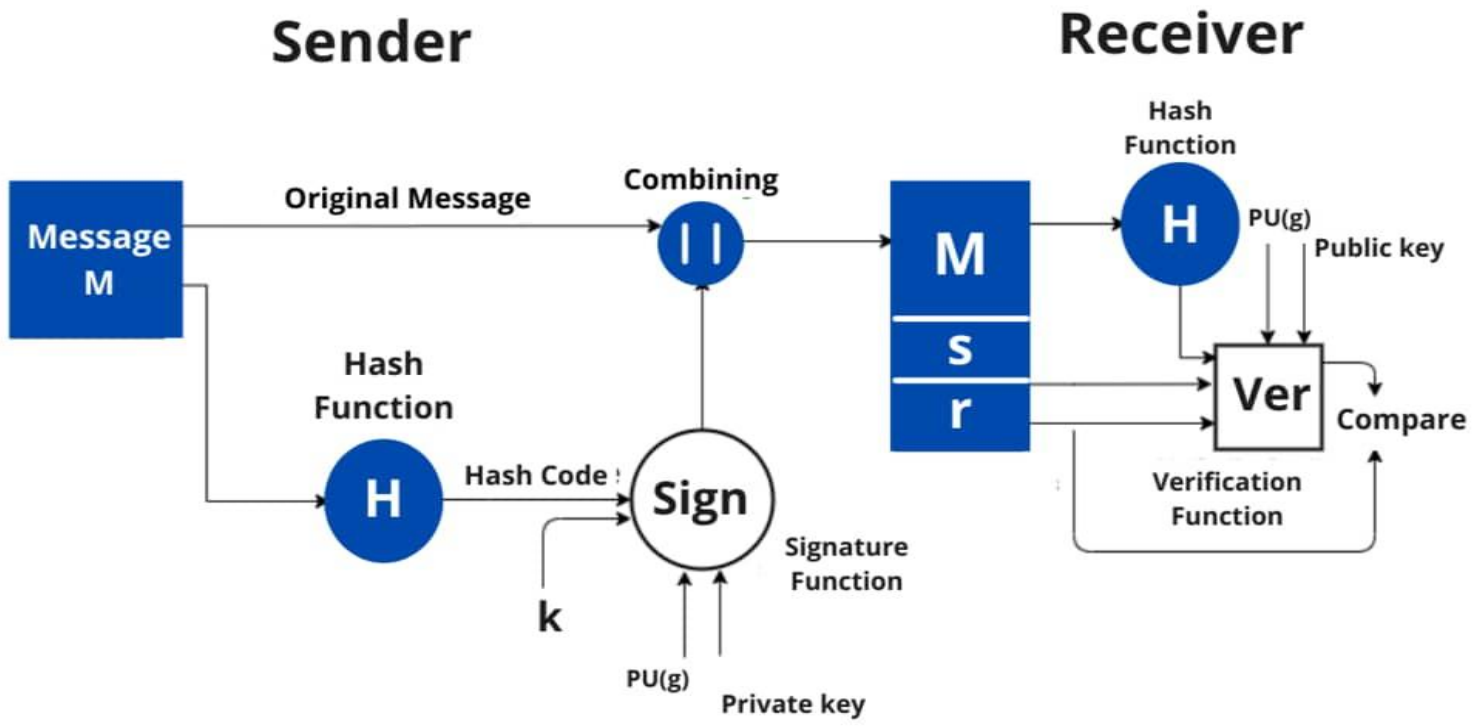
Two Tyes of Digital Signature

1. RSA Approach
2. DSS Approach

RSA Approach



DSS Approach



THANK YOU