Computer Security and Privacy (COM-301)

Week 6: Applied Cryptography

Interactive Problem Solving

A mystery dinner

Bob is organizing a mystery dinner. To each participant, he sends an e-mail with a role and a character story. Beforehand, each participant has generated a key pair and has sent their public key to Bob so that Bob can encrypt his e-mail to them.

Before the dinner, Bob wants to ensure that all participants have received their correct role. He asks participants to prove to him that they have received their correct role in a way that if somebody intercepts the mail from the participant to Bob they cannot learn the role assigned to the participant.

Unfortunately, Bob forgot to share his public key with the participants; so encrypting their mail is not an option. What primitive would you recommend that the participants use instead?

(a) A stream cipher

(b) An asymmetric cipher combined with Diffie Hellman

(c) A hash function with pre-image resistance

(d) A hash function

Cryptographic exchange

Alice
Public key: PKA

Bob
Public key: PKB

Alice generates a new symmetric key SK and sends to Bob: $E_{PKA}(SK), EPKB(SK), M \oplus Stream(IV, SK)$

Does the above exchange provide:

- Confidentiality
- Integrity
- Non-repudiation
- Or does not work because Bob cannot read M

where

$E_{PKB}(M)$ – public key encryption of M with public key PKB
$Stream(IV, SK)$ – stream of bits obtained from a stream cipher with key SK and initialization vector IV

Cryptographic exchange

Alice
Public key: PKA

Bob
Public key: PKB

Alice sends to Bob $E_{PKB}(SK1), AES_{SK1}(M), MAC_{SK2}(M)$

Does the above exchange provide:

- Confidentiality
- Integrity
- Non-repudiation
- Or does not work because Bob cannot read M

where

$AES_{SK1}(M)$ – Symmetric encryption of M with key $SK1$
$MAC_{SK2}(M)$ – Message authentication code with key $SK2$