Computer Security (COM-301)

Applied cryptography II

Interactive Exercises

Carmela Troncoso

SPRING Lab

carmela.troncoso@epfl.ch

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

Commit to avoid problems

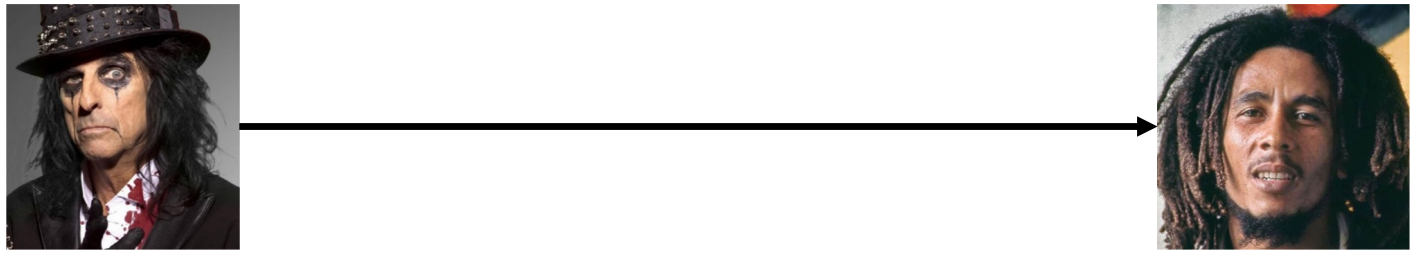
A commitment scheme is a cryptographic primitive that allows one to commit to a chosen value (i.e., one cannot change it later in time) while keeping it hidden from others, with the ability to reveal the committed value later.

A possible implementation of commitments is a hash function. To commit to the value 89, one provides Hash(89).

Imagine a case in which the professor commits to Joe Doe's score, imagine 60, in COM-301 and sends the commitment to central services. Since Joe is not happy with the score, he would like to convince central services that the score was higher.

When the professor chooses the hash function, what property/properties is needed to make sure that Joe Doe will not succeed?

Cryptographic protection



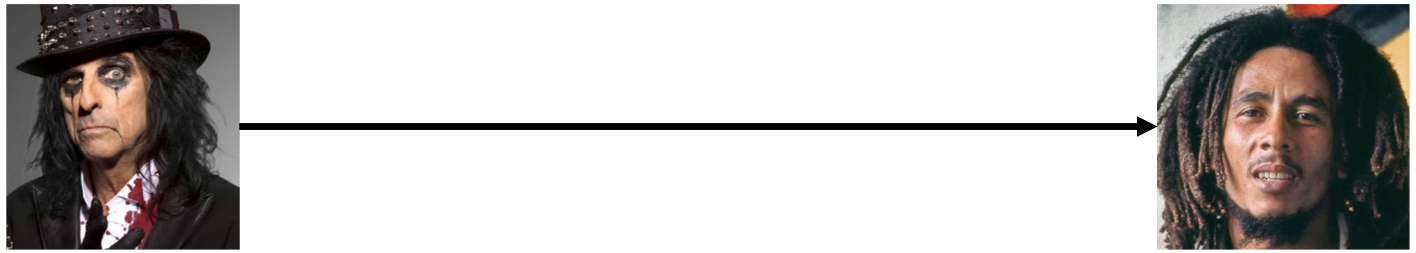
Does the following exchange provide:

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

Alice generates a new symmetric key *sk* and sends to Bob: $E_{PKA}(sk)$, $E_{PKB}(sk)$, M $\oplus$ *Stream(iv, sk)*

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

Cryptographic protection



Does the following exchange provide:

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

Alice sends to Bob $E_{PKB}(sk_1)$, AES(sk_1,M), MAC(sk_2,M)

AES(k,m) – symmetric encryption with key k

MAC(k,m) – Message authentication code with key k