CS3200: Computer Networks

Lecture 36

IIT Palakkad

13 Nov, 2019

Digital Signatures

- The authenticity of many legal, financial, and other documents is determined by the presence or absence of an authorized handwritten signature.
- For computerized message systems to replace the physical transport of paper-and-ink documents, a method must be found to allow documents to be signed in an unforgeable way.

Digital Signatures

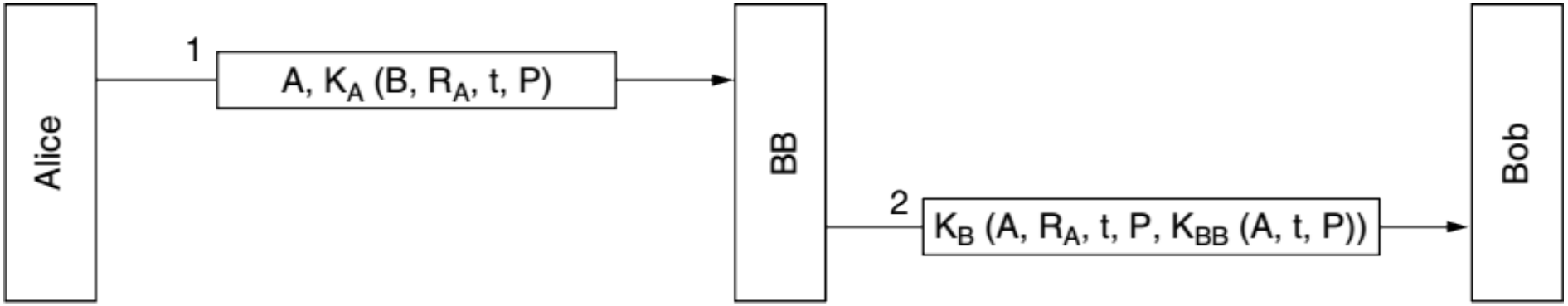
Basically, what is needed is a system by which one party can send a signed message to another party in such a way that the following conditions hold:

- The receiver can verify the claimed identity of the sender.
- The sender cannot later repudiate the contents of the message.
- The receiver cannot possibly have concocted the message himself.

concocted -> make a dish

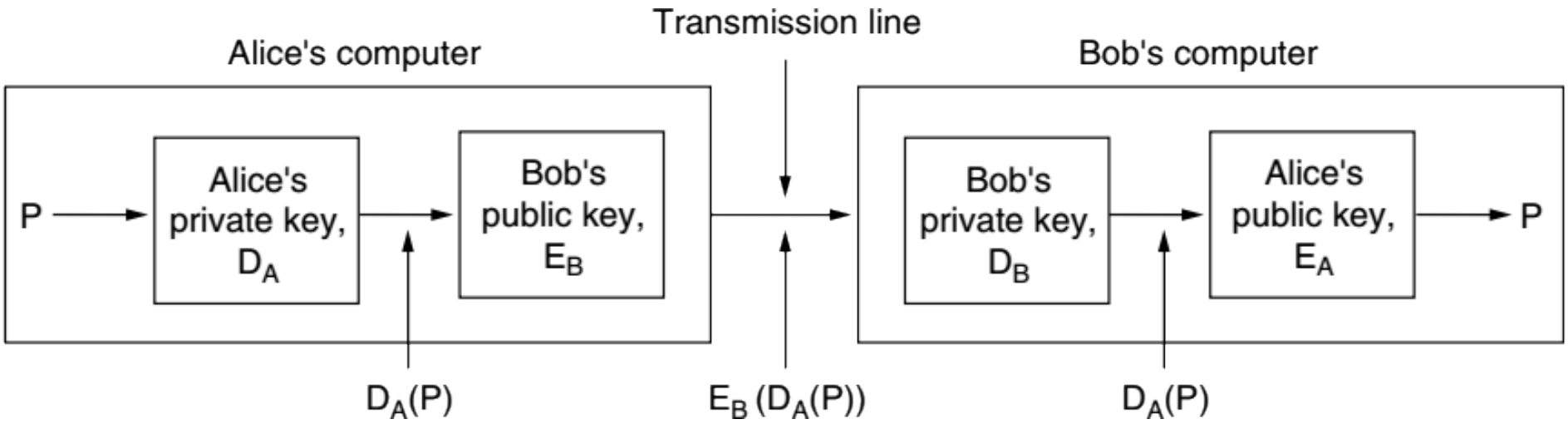
Symmetric-Key Signatures

We trust BB. BB Has everyone's private key. And nobody knows BB's private key.1) holds as BB verified that is it indeed alice and bob



Public-Key Signatures

1, 2, 3 all have same reason as end result P will have structure.



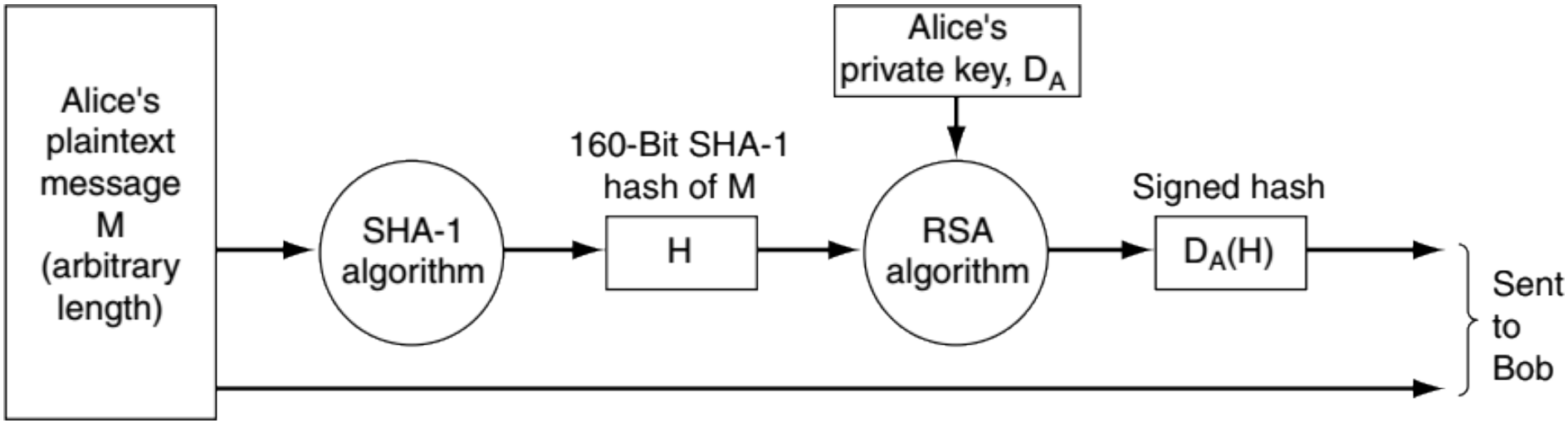
Message Digests

Our requirements don't insist to keep plain text private consequently plain text is kept public. Al

This scheme is based on the idea of a one-way hash function that takes an arbitrarily long piece of plaintext and from it computes a fixed-length bit string. This hash function, MD, often called a **message digest**, has four important properties:

1. Given P, it is easy to compute $MD(P)$.
2. Given $MD(P)$, it is effectively impossible to find P.
3. Given P, no one can find P' such that $MD(P') = MD(P)$.
4. A change to the input of even 1 bit produces a very different output.

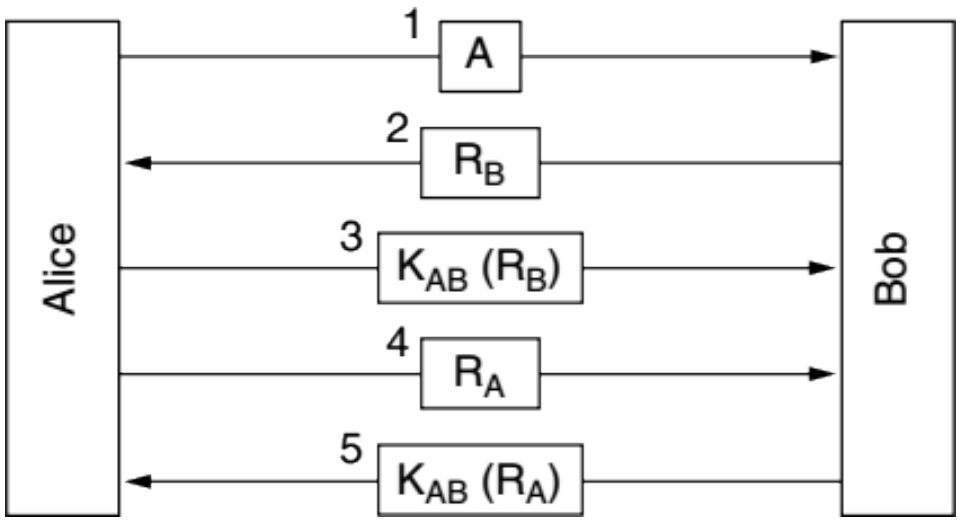
Message Digests



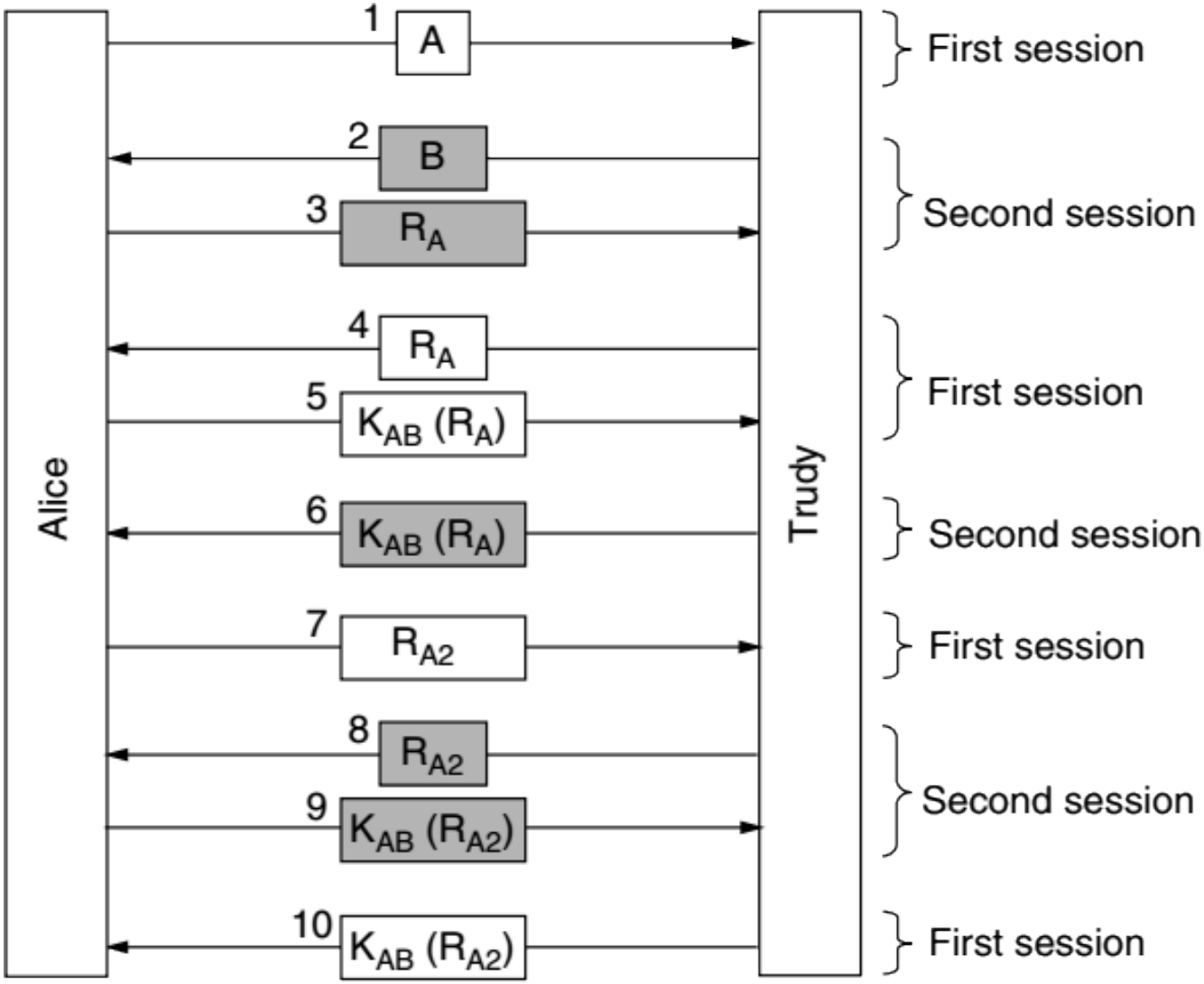
Authentication Protocols

- Authentication is the technique by which a process verifies that its communication partner is who it is supposed to be and not an imposter.
- Authentication deals with the question of whether you are actually communicating with a specific process. Authorization is concerned with what that process is permitted to do.
- Several messages are exchanged between Alice and Bob. As these messages are being sent, Eve may intercept, modify, or replay them in order to trick Alice and Bob or just to gum up the works.
- When the protocol has been completed, Alice is sure she is talking to Bob and Bob is sure he is talking to Alice.

Authentication Based on a Shared Secret Key

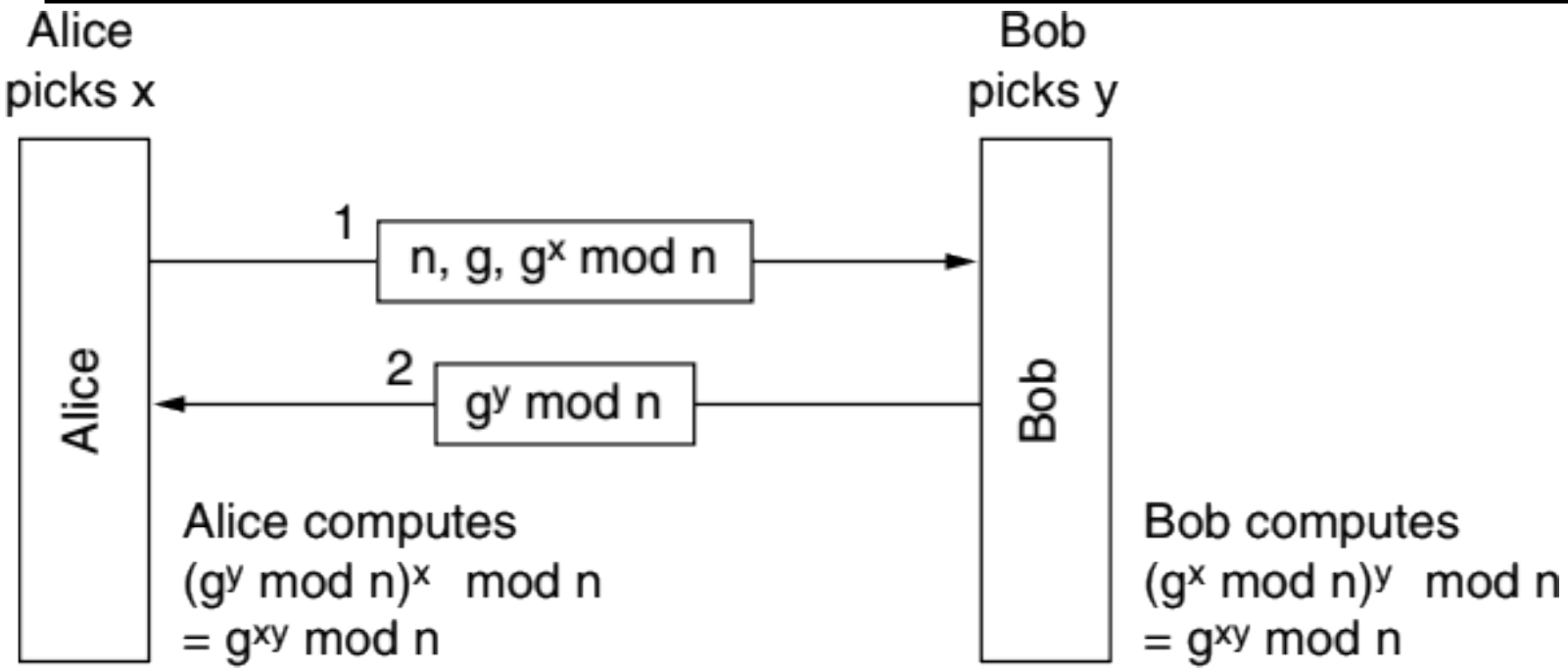


Reflection Attack



Establishing a Shared Key: The Diffe-Hellman Key Exchange

Alice and Bob have to agree on two large numbers, n and g, where n is a prime, (n 1)/2 is also a prime, and certain cor



Authentication Using Public-Key Cryptography

E = public key, Ks = shared key. side note for 6, random number helps in freshness.Side note for 7, same rand