Week 8: Applications of Cryptography I

Dr. Qublai K. Ali Mirza

University of Gloucestershire

qalimirza@glos.ac.uk

UNIVERSITY OF GLOUCESTERSHIRE

Overview

- While the current cryptography approaches can be used to protect sensitive data, we need some kind of mechanism to establish trust in terms of communication
- More specifically we want a mechanism that guarantees:
  - Message authentication
  - Integrity of message
  - Nonrepudiation
  - Confidentiality
- One of the mechanisms to this end are *digital signatures*

Digital signatures overview

Figure: Digital signatures overview

Overview

- A hash value is created for the email.
- The message with the hash is signed using the senders private key.
- The receiver decrypts the message using the senders public key.
- A hash is calculated for the message and compared to the sent hash.
- If OK, the message has not been modified.

Characteristics

- Provides the security properties of a signature in digital form, rather than written form
- Not designed to provide confidentially of the contents of a message
- Validates the sender and the contents of the message
- Implements asymmetric cryptography and hashing

Digital signature schemes

- There are a number of different digital signature schemes, but we will be focusing on:
  - RSA Digital Signature
  - Digital Signature Standard (DSS)

RSA Digital Signature

- Features the use of the RSA in key generation
- A *message digest* is first generated using an MGF function such as *SHA-1*
- The message digest is then encrypted using the sender's *private key*
- The message is deemed authentic if the decrypted MD is equal to the value obtained at the receiver's end

How RSA-DS works

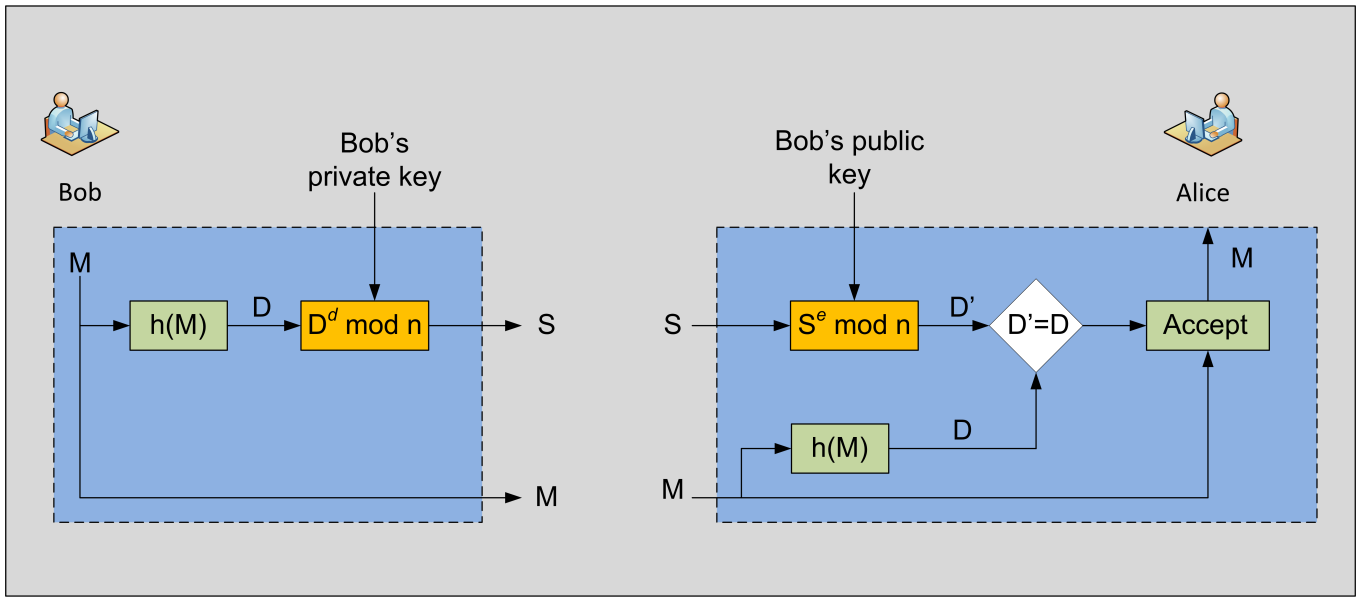

Figure: RSA Digital Signature operation, reproduced from [2]

Digital Signature Standard (DSS)

- Also features the use of a hash function together with public key encryption
- Features the use of the following additional components:
  - k: A pseduorandom that makes each digital signature unique
  - r, s: Functions based on the the recipient's public key, the sender's private key and the hash value of the message $H(M)$

DSS

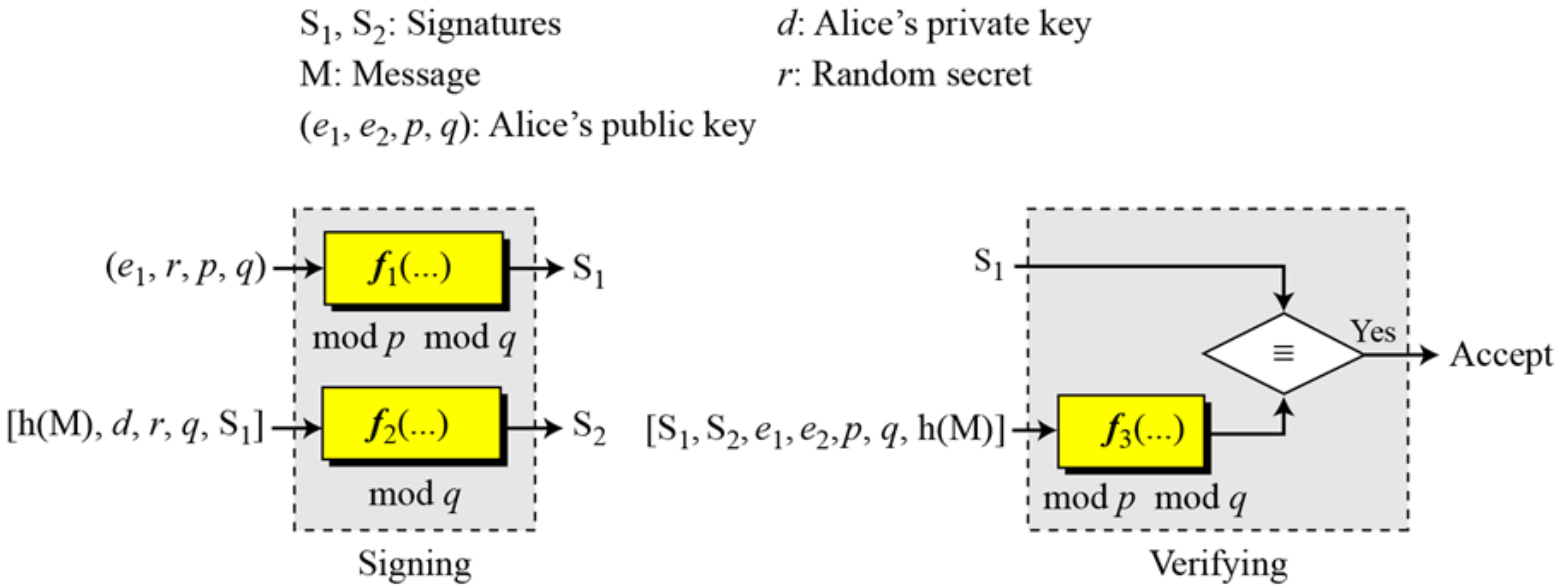

Figure: DSS operation, from [1]

Attacks against digital signatures

- Key-only attack
  - Based on the sender's public key
- Known-Message attack
  - Based on the knowledge of the messages and their corresponding signatures
- Chosen-Message attack
  - Independent of the knowledge of target's public key
  - The attacker first selects a group of messages
  - Then gets the target to generate corresponding signatures based on his/her private key

Overview

- So far we have looked at both:
  - Symmetric encryption
  - Asymmetric encryption approaches
- While public key encryption allows for a better protection, it also requires more computational power in key generation
- In addition, we would like to have the possibility to reuse the key pairs generated as well
- With that in mind, we need to look at how we can securely distribute *public* keys

Public key distribution

- Distribution of keys can be done using either:
  - Public announcement
  - Publicly available directory
  - Public-key certificates

Public announcement

- Public keys distributed openly to everyone through different means (e.g., publishing it on personal website, forums, etc)
- Tools such as *PGP* (Pretty Good Privacy) are used
- While it allows for ease of access, it opens up to the possibility of forgery
  - This can potentially lead to *masquerading* attacks

Publicly available directory

- Public keys are stored in a centralised directory which is publicly available
- The directory stores the public keys using *name*, *public key* pairs
- Requires registration from the user side
- Still vulnerable to tampering and/or forgery

Public key certificates

- A certificate that binds identity to public key
- Allows for exchange of keys without real-time access to *public key authority*
- Signed by a trusted *Certificate Authority* (CA)
  - Authorised to certify the identity

Public-key certificates

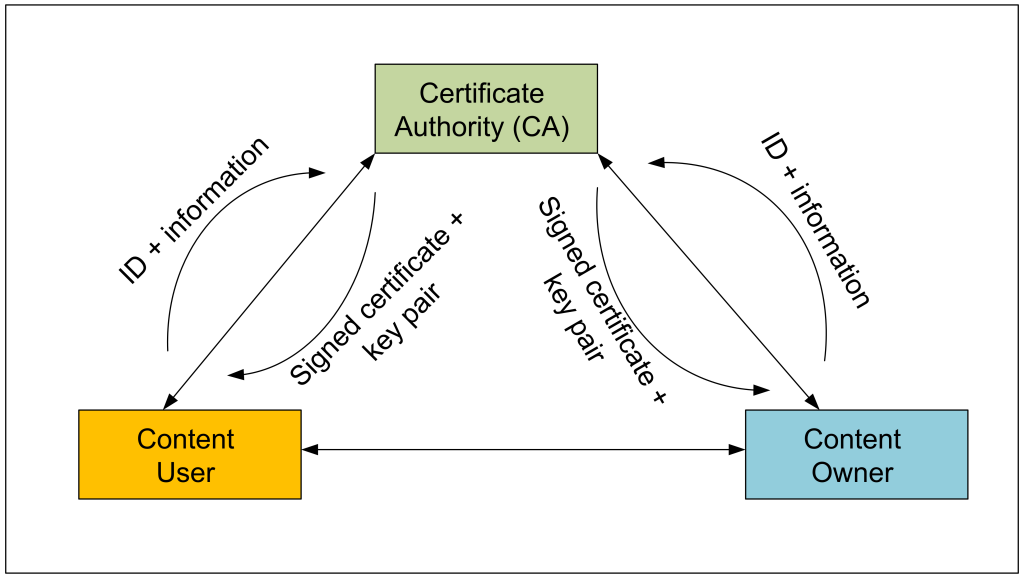

Figure: How public key cerificates work

Example Public-Key certificate

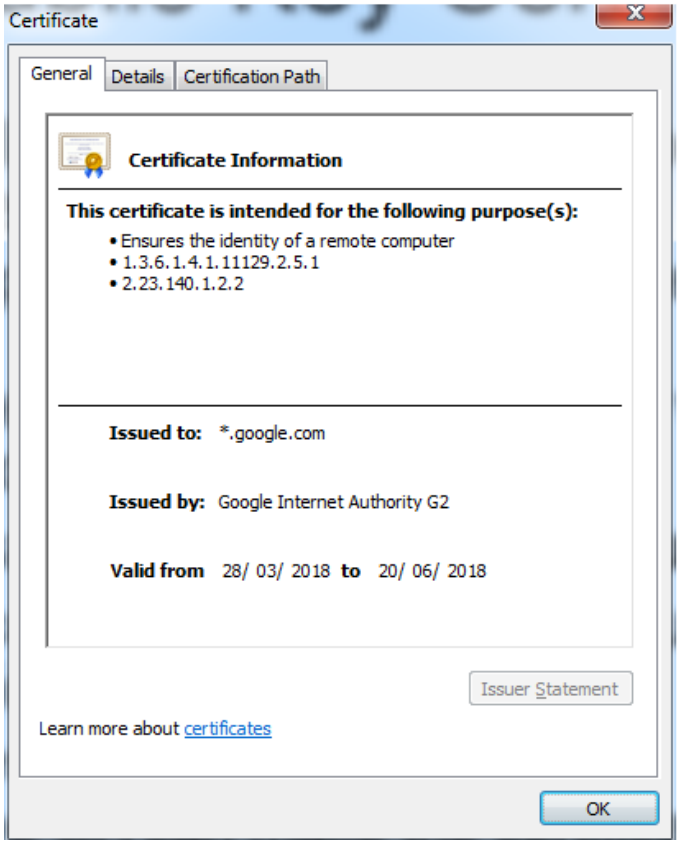

Figure: Sample public key certificate

Bringing it all together

- Today we looked at *applications of cryptography*
- We looked at how digital signatures work
- We also at key management and distribution
- Next week: *Applications of Cryptography II*

References I


Behrouz A Forouzan and Debdeep Mukhopadhyay. *Cryptography and Network Security (Sie)*. McGraw-Hill Education, 2011.


William Stallings. *Cryptography and network security: principles and practices*. Pearson Education India, 2006.

Q & A