Computer and Network Security
- Security Technology Part 2–
VER 2019

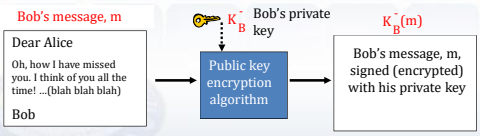
What is a digital signature?

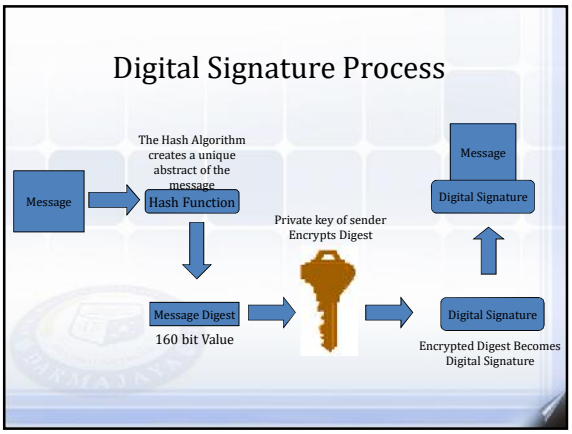
- is an **electronic signature** that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later.
- is a type of **asymmetric cryptography** used to simulate the security properties of a **signature** in digital, rather than written, form. Digital signature schemes normally give two algorithms, one for signing which involves the user's secret or **private key**, and one for verifying signatures which involves the user's **public key**. The output of the signature process is called the "digital signature."

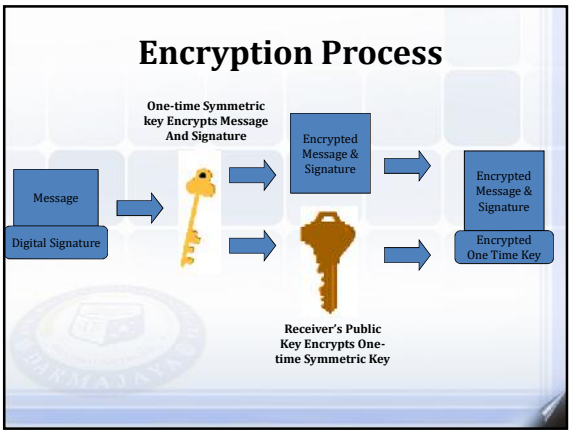
Digital Signature

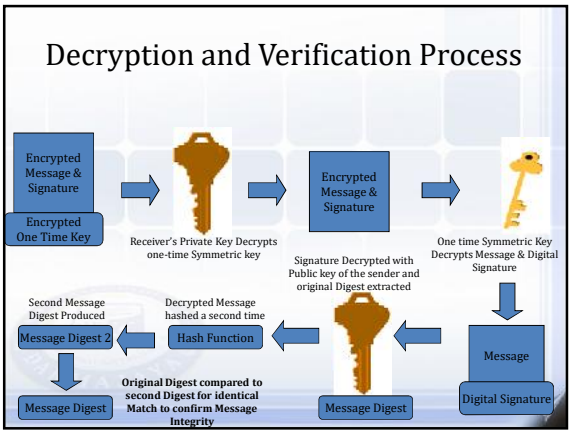
Example digital signature for message (m):

- Bob signs (m) by encrypting it with his private key (K_B^-), to produce signed message ($K_B^-(m)$)




Digital Signature Process
Message
The Hash Algorithm creates a unique abstract of the message
Hash Function
Message Digest
160 bit Value
Private key of sender Encrypts Digest
Digital Signature
Encrypted Digest Becomes Digital Signature
Message
Digital Signature


Encryption Process
One-time Symmetric key Encrypts Message And Signature
Message
Digital Signature
Encrypted Message & Signature
Encrypted Message & Signature
Encrypted One Time Key
Receiver's Public Key Encrypts One-time Symmetric Key


Decryption and Verification Process
Encrypted Message & Signature
Encrypted One Time Key
Receiver's Private Key Decrypts one-time Symmetric key
Encrypted Message & Signature
One time Symmetric Key Decrypts Message & Digital Signature
Signature Decrypted with Public key of the sender and original Digest extracted
Second Message Digest Produced
Message Digest 2
Decrypted Message hashed a second time
Hash Function
Message
Digital Signature
Message Digest
Original Digest compared to second Digest for identical Match to confirm Message Integrity
Message Digest

Benefits of digital signatures

These are common reasons for applying a digital signature to communications:

- **Authentication**

→ Although messages may often include information about the entity sending a message, that information may not be accurate. Digital signatures can be used to authenticate the source of messages.

→ When ownership of a digital signature secret key is bound to a specific user, a valid signature shows that the message was sent by that user.

→ The importance of high confidence in sender authenticity is especially obvious in a financial context. For example, suppose a bank's branch office sends instructions to the central office requesting a change in the balance of an account. If the central office is not convinced that such a message is truly sent from an authorized source, acting on such a request could be a grave mistake.

Benefits of digital signatures

- **Integrity**

→ In many scenarios, the sender and receiver of a message may have a need for confidence that the message has not been altered during transmission. Although encryption hides the contents of a message, it may be possible to *change* an encrypted message without understanding it.

→However, if a message is digitally signed, any change in the message will invalidate the signature. Furthermore, there is no efficient way to modify a message and its signature to produce a new message with a valid signature, because this is still considered to be computationally infeasible by most cryptographic hash functions.

Another Issue

- in-person" verification can be done in a matter of seconds, and becomes a routine affair. However, replicating this procedure on-line is more difficult. The on-line version can't visually compare your face to your ID, nor compare your signature to the previously approved government-sanctioned version of your signature.
- So what is needed is an on-line mechanism that provides a similar sort of assurance from an authority that can say, essentially "you don't know this guy, but I do, and he's okay by me".

How To Overcome

- That authority in the on-line environment is known as a "certificate authority" (CA), an agency whose integrity must be beyond reproach.
- A certificate authority establishes protocols to ascertain the identity of registrants, and supports on-line verification that the identity has been proven to the CA. The Certificate Authority essentially says "I checked this person out, and verified that he is who he says he is, you have my word on it".
- To acquire a digital certificate, an individual or organization registers with a certificate authority and presents proof of identity. The CA requests specific information of the registrant, investigates it, and then issues a digital certificate that confirms that the CA has verified the information independently.

Digital Certificate

The certificate would typically include the following information:

- The registrant's name
- Additional personal information such as an e-mail address for a person or a URL for a web server
- A unique registration number
- The name of the certificate authority
- The public key of the registrant
- Dates that reflect certificate validity (start and expiration dates)
- A digital signature "seal" from the CA that verifies authenticity of the certificate

Certification Authority

- Kriptografi kunci publik dapat digunakan untuk mengenkripsi data yang dikomunikasikan antara dua pihak. Ini biasanya terjadi ketika pengguna log on ke situs yang mengimplementasikan protokol HTTP yang aman (HTTPS).
- Dalam contoh ini mari kita anggap bahwa pengguna log on ke situs bank-nya www.bank.example untuk melakukan online banking. Ketika pengguna membuka situs www.bank.example, ia menerima kunci publik bersama dengan semua data yang menampilkan web-browser-nya.
- Kunci publik dapat digunakan untuk mengenkripsi data dari klien ke server
- Hanya server bank yang memiliki kunci pribadi untuk membacanya.

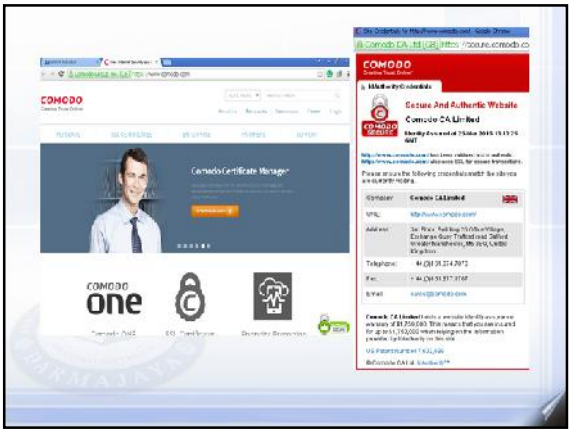
Certificate Authority

- Komunikasi berikutnya akan menggunakan kunci simetris baru (sekali pakai)
  - jadi ketika pengguna memasukkan beberapa informasi ke halaman bank mengirimkan informasi kembali ke bank maka data pengguna telah masuk ke halaman akan dienkripsi oleh web browsernya . Oleh karena itu, bahkan jika seseorang dapat mengakses (dienkripsi) data yang dikomunikasikan dari pengguna untuk www.bank.example, eavesdropper seperti tidak bisa membaca atau memahaminya.
- www.bank.example yang palsu dpat menggunakan kunci public yang sama, tetapi tidak akan mengetahui pasangan kunci privatenya,. Sehingga tidak dapat menghasilkan "signature" yang sesuai untuk proses autentikasi.

Digital Certificate

Token


mandiri
e-Secure
BCA


COMODO
Comodo Certificate Manager
COMODO
one
COMODO
Secure And Authentic Website
Comodo CA Limited

Serangan Cryptanalysis

- Replay Attack
  - Mengulangi nilai yang sudah diketahui sebelumnya.
- Social Engineering
  - Manusia adalah “link” terlemah
- Temporary Files
  - Mungin saja terdapat plaintext file

Serangan Cryptanalysis

- Ciphertext-Only
- Known Plaintext
- Chosen Plaintext
- Chosen Cipher text

Table 2.1 Types of Attacks on Encrypted Messages

Type of Attack	Known to Cryptanalyst
Ciphertext only	• Encryption algorithm • Ciphertext to be decoded
Known plaintext	• Encryption algorithm • Ciphertext to be decoded • One or more plaintext–ciphertext pairs formed with the secret key
Chosen plaintext	• Encryption algorithm • Ciphertext to be decoded • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen ciphertext	• Encryption algorithm • Ciphertext to be decoded • Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen text	• Encryption algorithm • Ciphertext to be decoded • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key • Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

Secure Encryption

- An encryption scheme is **computationally secure if the ciphertext generated** by the scheme meets one or both of the following criteria:
  - The cost of breaking the cipher exceeds the value of the encrypted information.
  - The time required to break the cipher exceeds the useful lifetime of the information.

At the end

The mantra of any good security engineer is: **'Security is a not a product, but a process.'** It's more than designing strong cryptography into a system; it's designing the entire system such that all security measures, including cryptography, work together.

by Bruce Schneier

End