




9.3 Computer and Network Security

Digital Signatures

INFO1112

Bob Kummerfeld

For network connections we wish to provide:

- **Confidentiality**
 - Protecting information from interception
 - Ensure information remains confidential if intercepted
- **Integrity**
 - Detecting whether information has been tampered with
-  **Authenticity**
 - Ensuring we know who the sender is
 - Non-repudiation

Authenticity - Digital Signature

If D and E can operate in either order (RSA has this property)
 $D(E(m)) = m = E(D(m))$ then they can be used to "sign" a message.

If Alice wants to prevent forgery of a message,
combine message m with $h = D(m, K_{\text{PRIV},A})$

Bob can check that m corresponds to this signature, by seeing
whether $m = E(h, K_{\text{PUB},A})$

ie Bob can prove that Alice sent the message, since only Alice has the private key necessary.

Combine signature and encryption to protect against both interception and forgery

Alice

The quick brown fox jumped over the lazy dog

plaintext

D(plaintext, Alice's **PRIVATE** key)

signature

7d38b5cd25a2baf85ad3bb5b9311383e67....

The quick brown fox jumped over the lazy dog

E(signedtext, Bob's **PUBLIC** key)

signed,
encrypted

5ad3bb5b9311387d38b5cd25a2baf85ad3bb5b9311383e67....



5ad3bb5b9311387d38b5cd25a2baf85ad3bb5b9311383e67....

D(signedtext, Bob's **PRIVATE**
key)

signature

7d38b5cd25a2baf85ad3bb5b9311383e67....

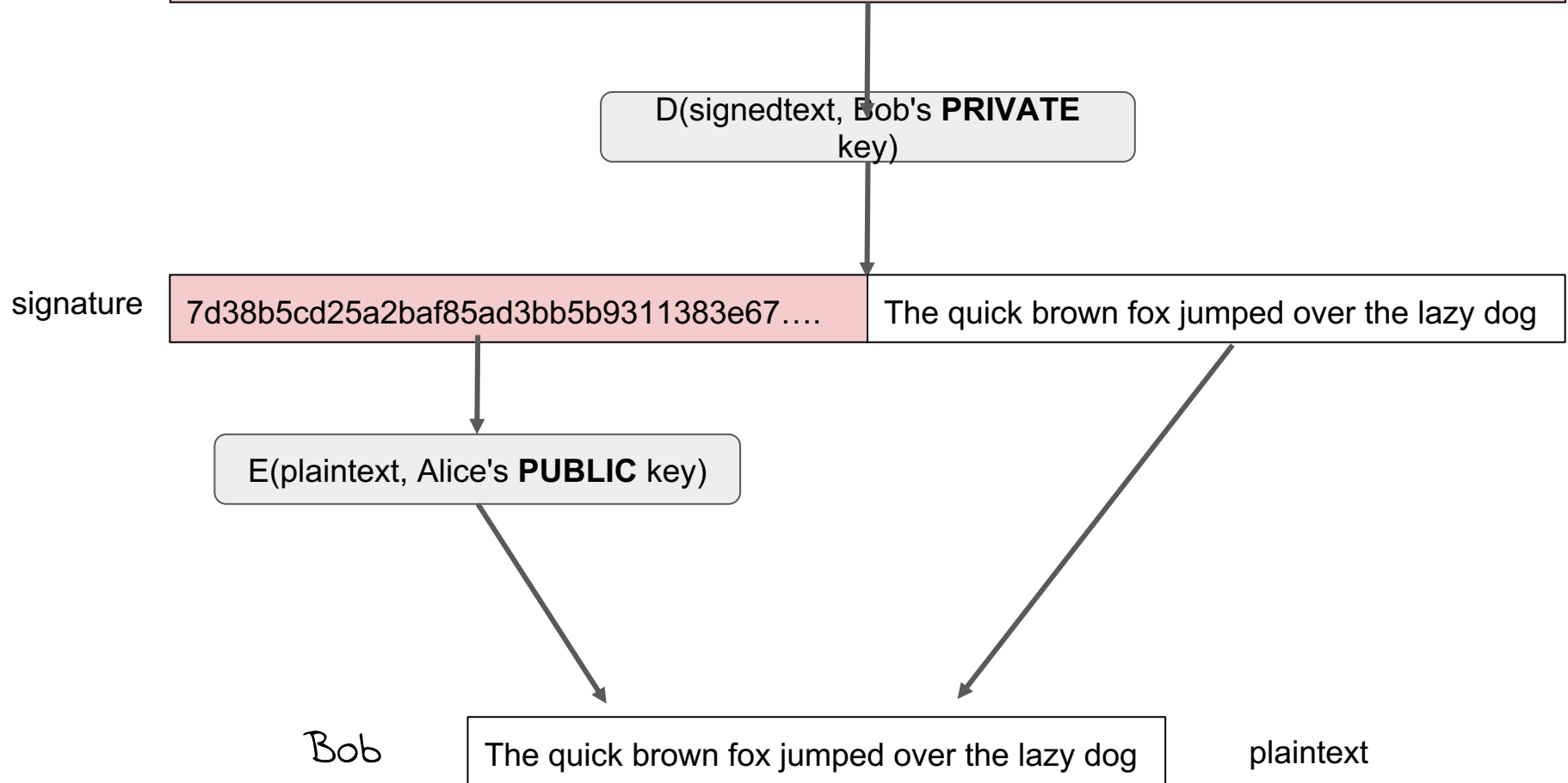
The quick brown fox jumped over the lazy dog

E(plaintext, Alice's **PUBLIC** key)

Bob

The quick brown fox jumped over the lazy dog

plaintext



Key establishment

Public key crypto is much slower than conventional shared secret crypto. For any arbitrary pair of users to communicate securely and with trust using conventional (shared secret) crypto we can do the following:

Alice can choose a key value (could be random), and send it to Bob encrypted with Bob's public key and signed with Alice's secret key

- the key value is a secret they share: they both know the value, but interceptor Carol doesn't know it

The shared secret can then be used in conventional symmetric cryptography

Public key infrastructure

How can we protect the information about Bob's public key from attack, and get it securely to Alice (establish trust)?

- Modification attack: if attacker can change the website where Bob's public key is stored, and put a different value there
 - Attacker could then read messages intended for Bob
 - Attacker could prevent Bob reading messages intended for him (denial of service)

Bob can pass his public key to Alice through trusted intermediaries

or Bob can prove his identity to a mutually trusted third party, who issues a *certificate* that links the public key with their statement that they have been convinced of Bob's identity

Digital Certificates

A digital certificate is a data structure that certifies the ownership of a public key by a named subject

- This allows others to rely upon signatures or on assertions made by the private key that corresponds to the certified public key.

Certificates are managed by "certificate authorities" that are trusted organisations. Certificates are signed by the secret key of the certificate authority and can be checked using the public key.

To protect the public key of the certificate authority a certificate is issued by a higher level authority

HTTPS Example

When you request a web page using a url starting with HTTPS the web server sends a public key to the browser in the form of a signed certificate.

This key is checked using the public key of the certificate authority (browsers usually store these locally)



SSH

SSH or Secure Shell is a program available on all Unix systems for secure communication.

SSH has its own communications layer above TCP/IP that provides encrypted login sessions and other services.

The simplest use of SSH is to provide a confidential session between unix systems. The authentication is handled in the usual way with login program asking for a password.

SSH can also be configured to use public key cryptography if a user stores their public key on the remote system and then uses their private key to encrypt a message for authentication.



SCP

SCP or Secure CoPy is a feature of SSH that allows a user to securely copy a file from one machine to another.

The user can use password authentication or public key authentication and SSH will send the file to the SSH server on the remote machine. A user can also copy a file *from* a remote machine securely.



SSH services

SSH is also used to provide a number of services where it is acting as a secure carrier for other protocols.

For example, the X11 display protocol can be used over SSH and provide remote window sessions to Unix/X11 based system.

SSH can also be used for ***tunnelling*** lower level protocols. This is where SSH effectively acts as a pipe for any protocol and so can carry TCP/IP (so this is TCP/IP over SSH over TCP/IP!).

This is useful for Virtual Private Network connections.

Final words...

Computer Security is a BIG and important topic. This has been a very brief introduction to some important aspects (symmetric and asymmetric cryptography, public key systems, public key infrastructure, secure hash, practical systems: https, ssh).

The School of Computer Science has a range of further courses in computer security, starting in second year.

Computer security has both technology aspects **and** human aspects. Both are important.

A CRYPTO NERD'S
IMAGINATION:

HIS LAPTOP'S ENCRYPTED.
LET'S BUILD A MILLION-DOLLAR
CLUSTER TO CRACK IT.

NO GOOD! IT'S
4096-BIT RSA!

BLAST! OUR
EVIL PLAN
IS FOILED!



WHAT WOULD
ACTUALLY HAPPEN:

HIS LAPTOP'S ENCRYPTED.
DRUG HIM AND HIT HIM WITH
THIS \$5 WRENCH UNTIL
HE TELLS US THE PASSWORD.

GOT IT.

