

Introduction to Cryptography

Public-key Infrastructures

Jean-Sébastien Coron

January 2007

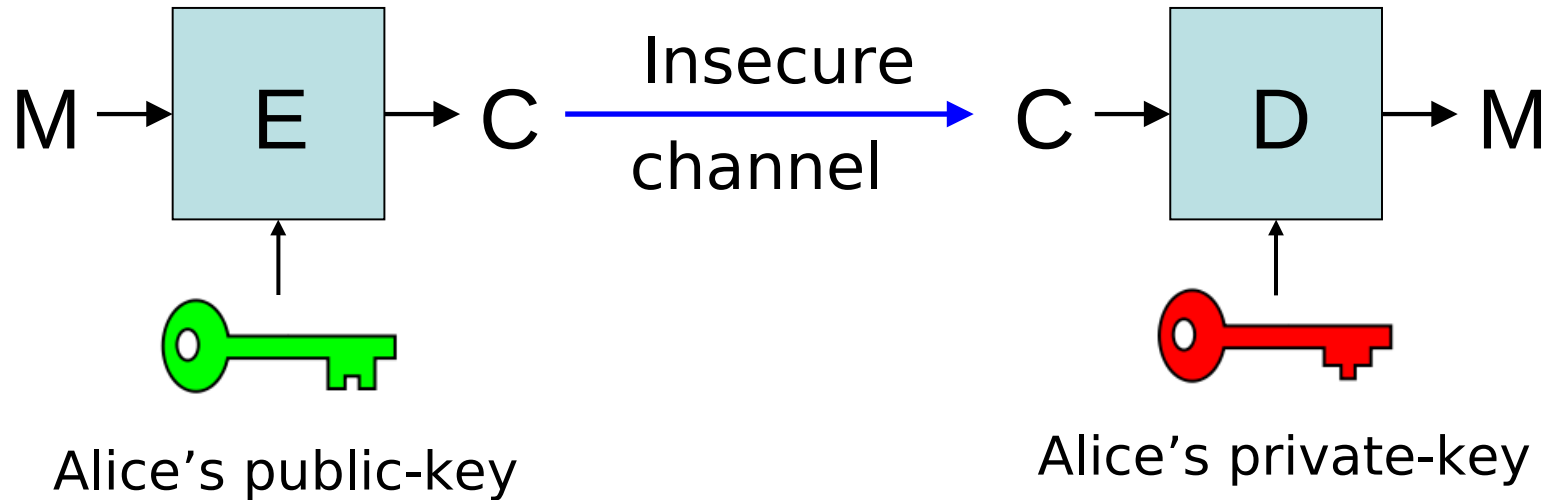
Public-key encryption



BOB

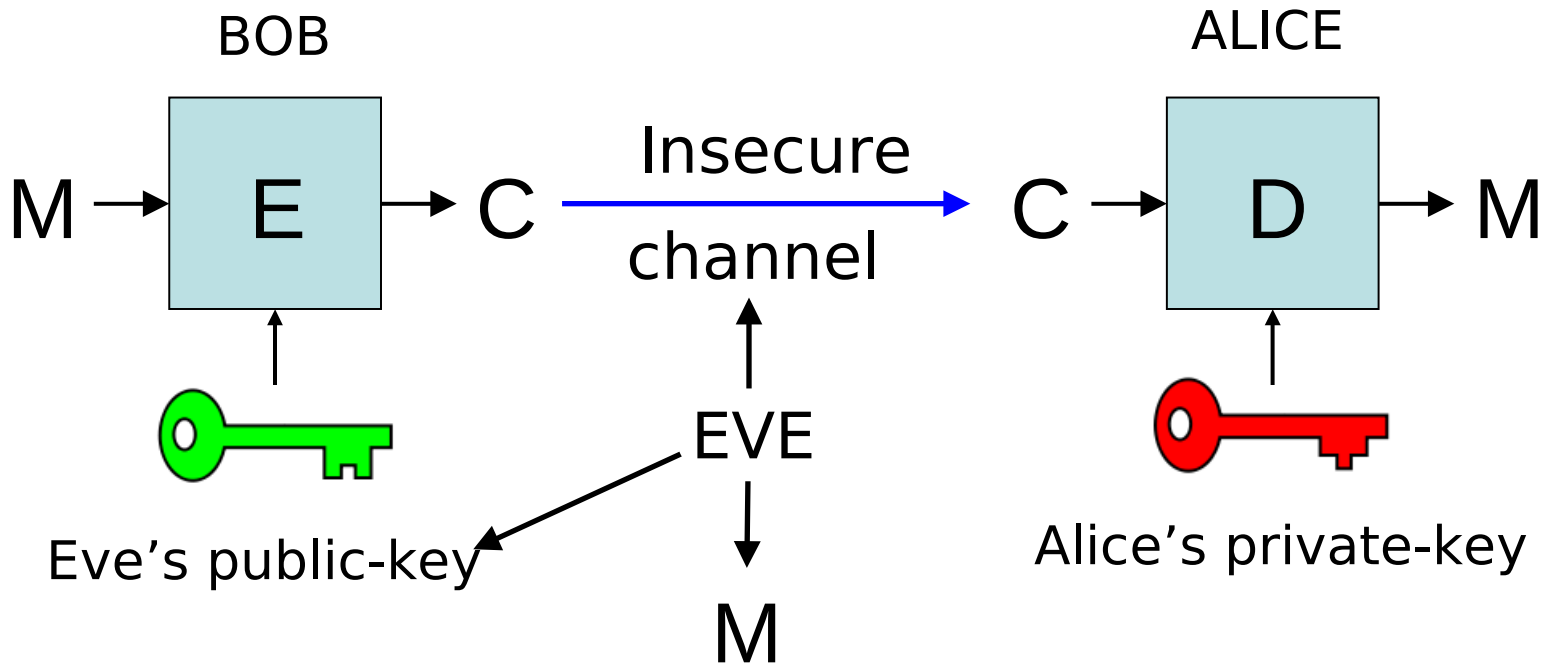


ALICE



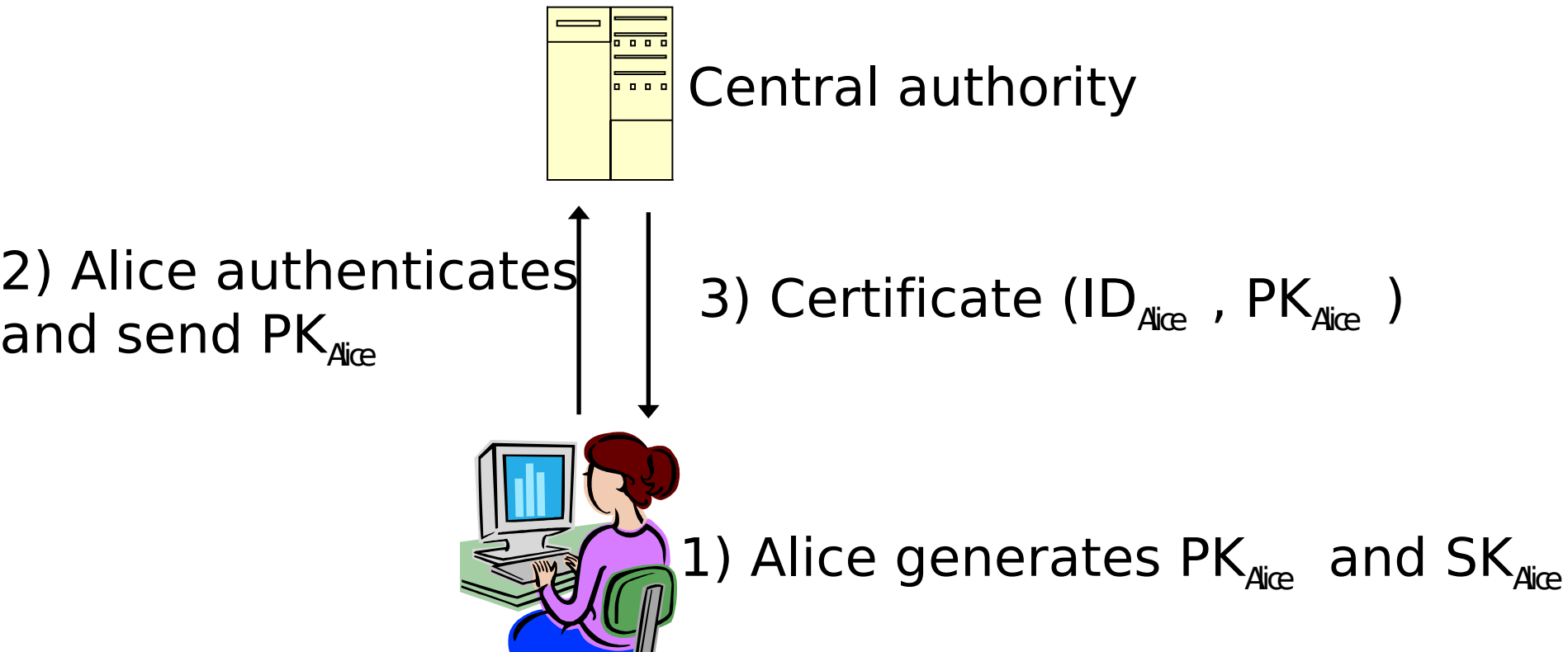
Authentication

- Public-keys need to be authenticated
 - Bob needs to be sure that the public-key belongs to Alice.
 - Otherwise, impersonation attack



Public-key Infrastructure

- A central authority binds public-keys to identities.
 - Public-key is stored in a certificate



Public-key certificate

- Certificate:
 - the signature of the certificate authority binds together a public-key with an identity.
 - Bob can be sure that the public-key belongs to Alice by checking the signature using the CA public-key.
 - The CA is trusted by all participants.

Certificate Authority

- CA issues PK certificates that attest that the PK in the certificate belongs to the identity in the certificate
 - CA must verify user's identity before issuing certificate
 - If the CA's private key is compromised, security is lost.
- Largest providers of certificates
 - Verisign, Geotrust

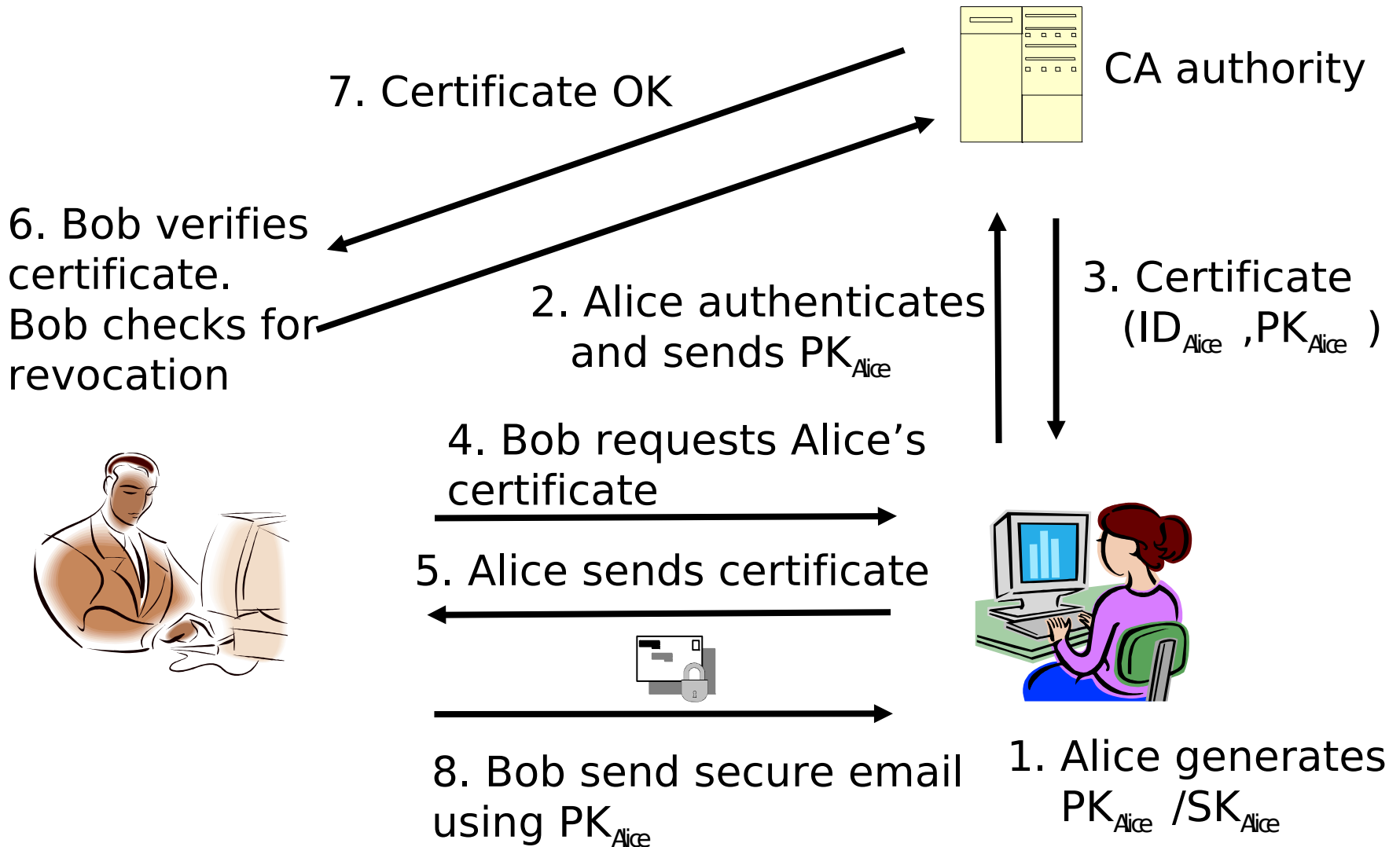
Public-key certificate

- A public-key certificate may include
 - user's public-key
 - name (person, computer, or company)
 - validity period.
 - location (URL) of a revocation center.
 - digital signature of the certificate, produced by the CA's private key.

Certificate revocation

- Certificate revocation when
 - Private-key is compromised
 - Identity/PK binding incorrect.
- A user should always check the validity of a certificate
 - CA can maintain a Certificate Revocation List (CRL)
 - Must be up to date and readily available

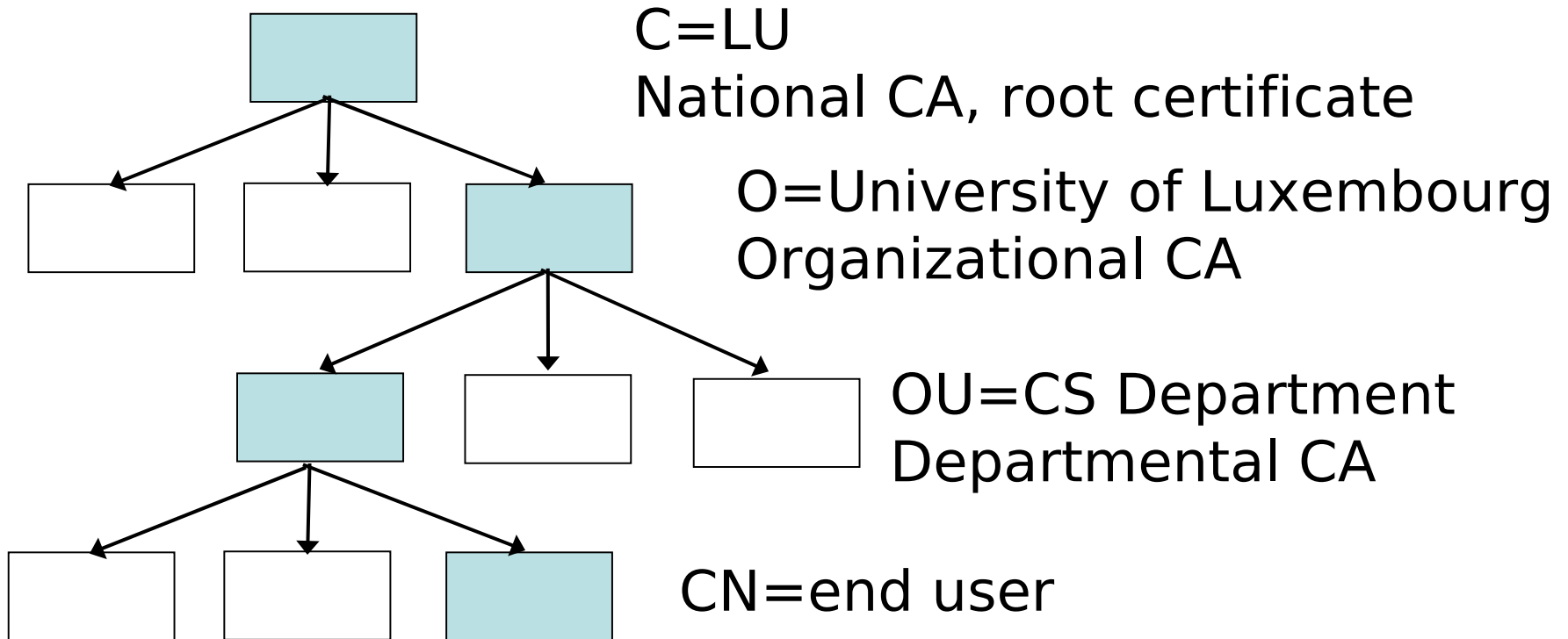
PKI encryption



Hierarchy of certificates

- Bob may not know Alice's CA
 - The CA may be Alice's employer, and Bob may work for a different company.
- Alice's certificate can include her CA's public-key signed by a higher level CA₂
 - This CA₂ may be recognized by Bob
- This leads to a hierarchy of certificates

Certificate Hierarchy



Certificate Standard

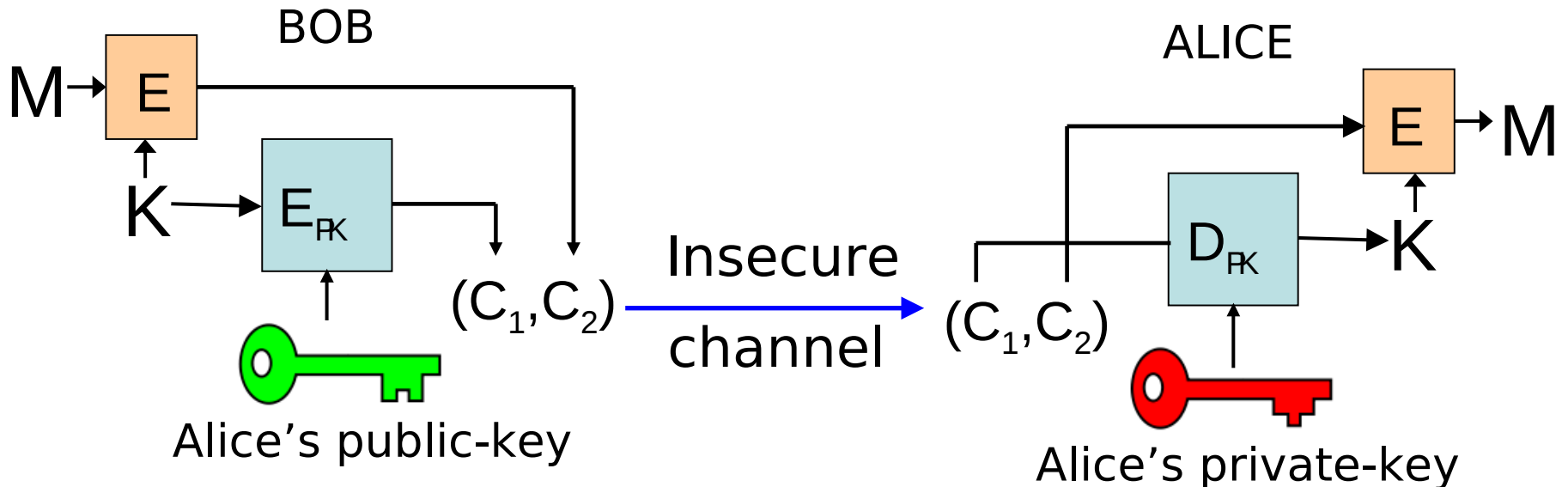
- X509
 - Most common certificate standard
 - Specifies certificate format and certificate validation path.
 - Assumes a hierarchy of CA
 - Root certificate is implicitly trusted
 - Specifies certificate revocation list (CRL) implementation

Root certificate

- Unsigned public-key certificate located at the top of a certificate chain.
 - Typically in X509 standard
 - Implicitly trusted
- Included in web browsers
 - Used for SSL/TLS connections
 - One needs to trust the browser's publisher to include correct root certificates.
 - Single point of failure
- In practice, hierarchy is flat.

PGP

- PGP (Pretty Good Privacy)
 - Software that provides email encryption and signature (and more).
 - First version by P. Zimmermann in 1991.
 - Uses PK encryption to encrypt a shared key, which is used to encrypt the message.

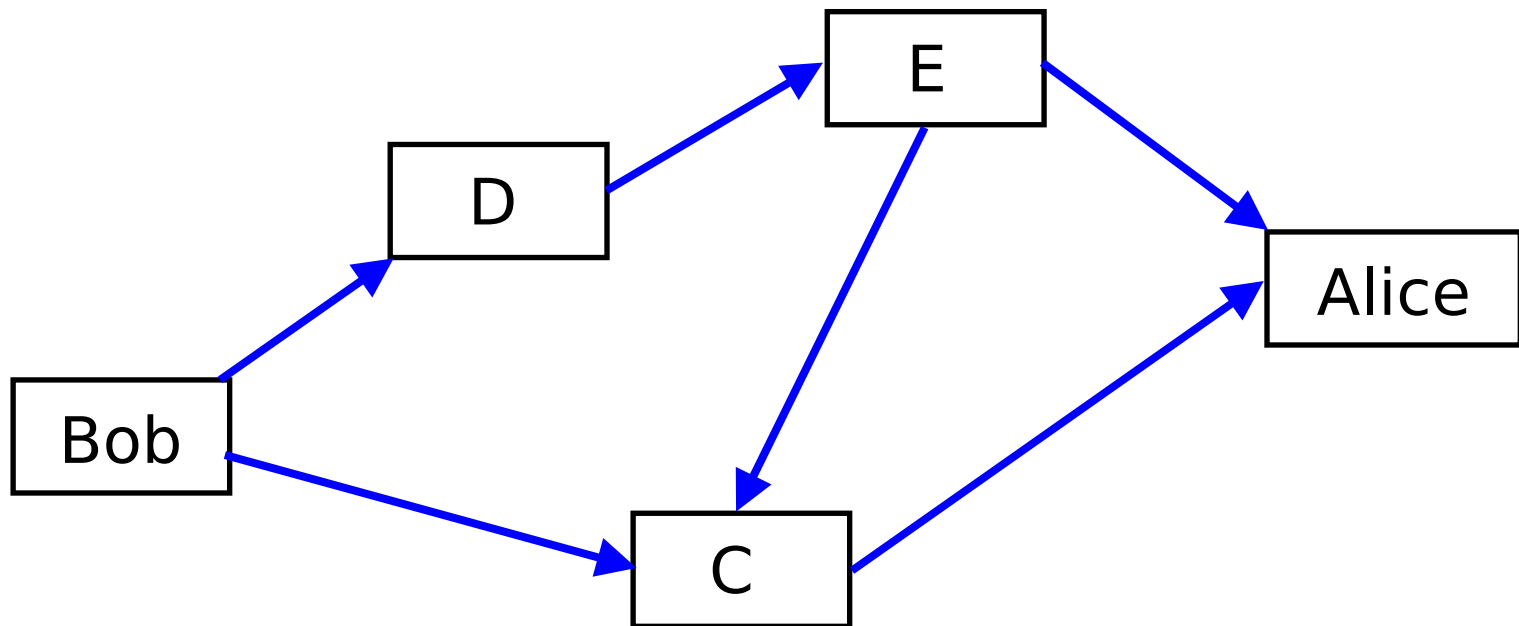


PGP

- Digital signature
 - When sending a message m , Bob can sign m with his private key.
 - Alice checks the signature with Bob's PK, so that Alice is convinced that m was sent by Bob and received unaltered.
 - RSA signature or DSA signature.
 - Used by default with encryption, but can be used for plaintext as well

PGP Web of trust

- Any party can sign the (PK, ID) of another.
- Decentralized web of trust



OpenPGP and GnuPG

- OpenPGP
 - Standard for PGP encryption since 1997.
 - Avoids patented algorithms
- GNU Privacy Guard (GnuPG)
 - developed by Free Software Foundation and freely available with source code.
 - Supports ElGamal, DSA, RSA, AES, 3DES, Blowfish, Twofish, CAST5, MD5, SHA-1, RIPE-MD-160 and TIGER.

SSL

- Used to provide secure web-browsing.
 - SSL 3.0 similar to TLS 1.0
 - ensures confidentiality, integrity and authenticity over the Internet.
- Generally, only the server is authenticated
 - Mutual authentication requires a PKI for the client.

SSL

- Three steps
 - Negotiation for algorithms used.
 - Certificate verification and PK encryption for session key.
 - Symmetric encryption for traffic encryption.

Cipher suite negotiation

- Client sends a ClientHello message to specify supported algorithms
 - For example, RSA, AES and HMAC-SHA-1
- Server sends a ServerHello message to specify its choice of algorithm.
 - Server adapts to client capabilities.

SSL: second phase

- Server sends certificate to client.
 - Generally, X509 certificate
- Server can request client certificate for mutual authentication
 - Rarely used in practice
- Client and Server establish a « master secret »
 - by PK encryption of a random seed by the client (generally RSA)
 - or possibly by Diffie-Hellman key exchange (rarely used)

SSL second phase (2)

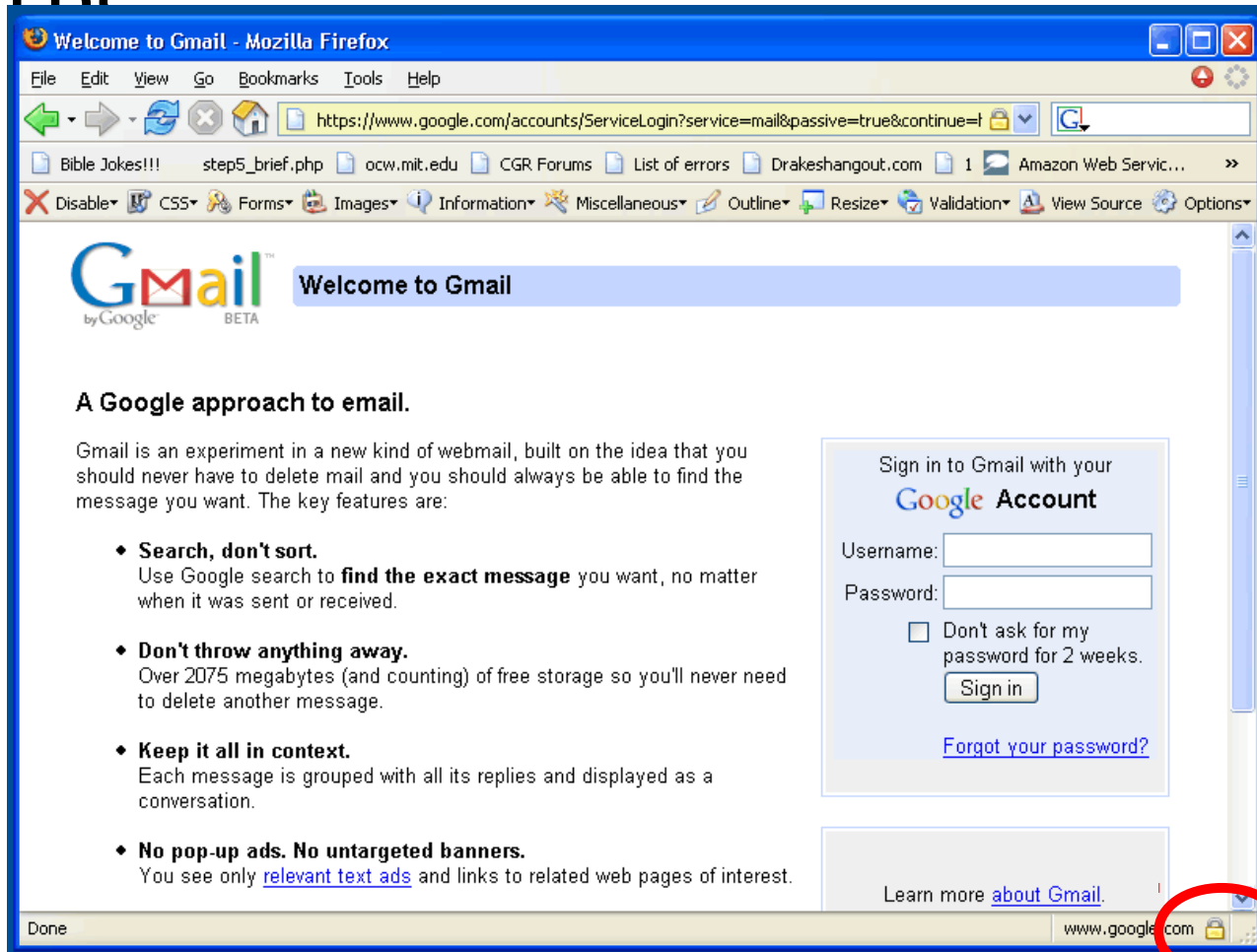
- Server authenticated by proof of possession of private key
 - Ability to decrypt client data.
 - Both sides share the same « master secret »
- Client/server finish
 - Authenticate all previously exchanged data with MACs

SSL: third phase

- Traffic encryption
 - Using symmetric cipher
 - Some early implementations of SSL used 40-bit keys because of US government restrictions on crypto export
 - Now relaxed export restrictions. Modern implementations use 128 bit keys for symmetric key.
- Integrity protection via MACs

Applications of SSL

- Mainly used to secure HTTP => HTTPS



Credit card via https

- https only protects the credit card number during transit between the user's computer and the server
 - Does not protect against an attack on the server
- Attack on the server usually easier than interception in transit.
 - Credit card number often saved in a database in merchant site
 - Attacks generally concentrate on the server and database

Conclusion

- Public-key Infrastructure
 - Necessary to authenticate public-keys
 - Difficult to set up and maintain
 - Certificate Revocation List
 - Used for PGP encryption and SSL/TLS.