Internet Security

Putting together the building blocks...

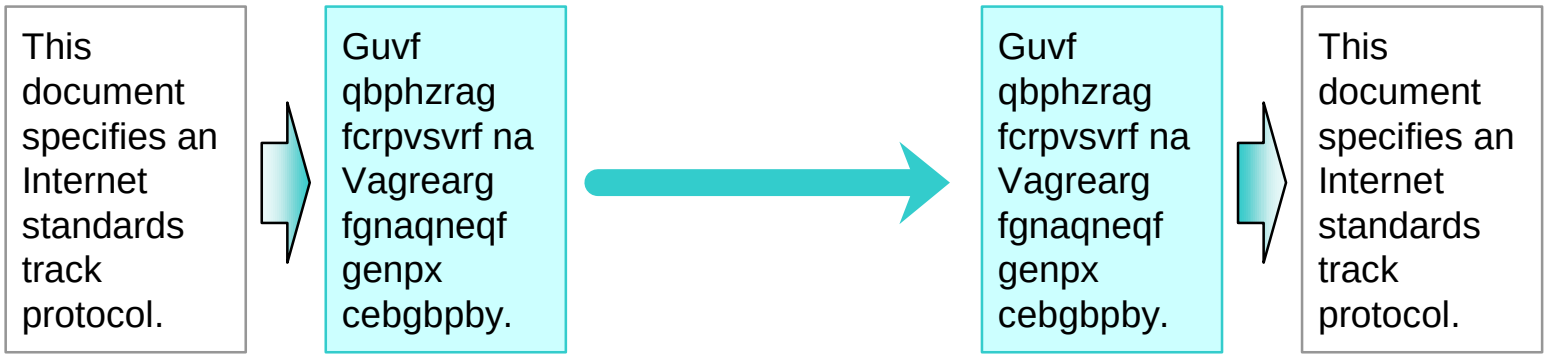
Maximilian Riegel

Agenda

- Basic cryptography
  - Hash functions
  - Secret key cryptography
  - Public key cryptography
- Providing identity
- Verifying information
- Keeping secrets
- Key management
- Internet security protocols

Basic Cryptography

- "Cryptography" originates from Greek for "secret writing"
- Keeping information secret is often associated with cryptography.



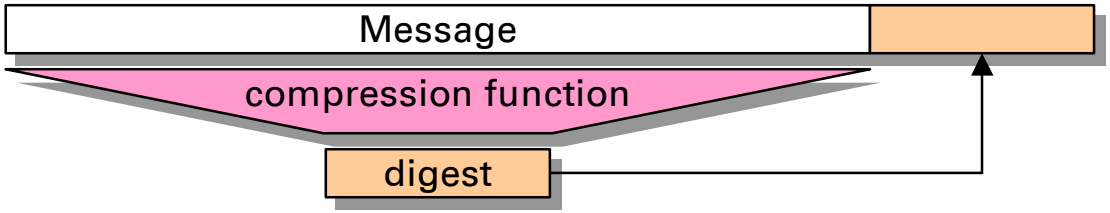
Important uses of cryptography to gain security

- Confidentiality - *keeping secrets against eavesdropping*
- Authentication - *providing identity against forgery and masquerade*
- Message integrity - *verifying information against alteration*

Cryptography is no means against denial of service!

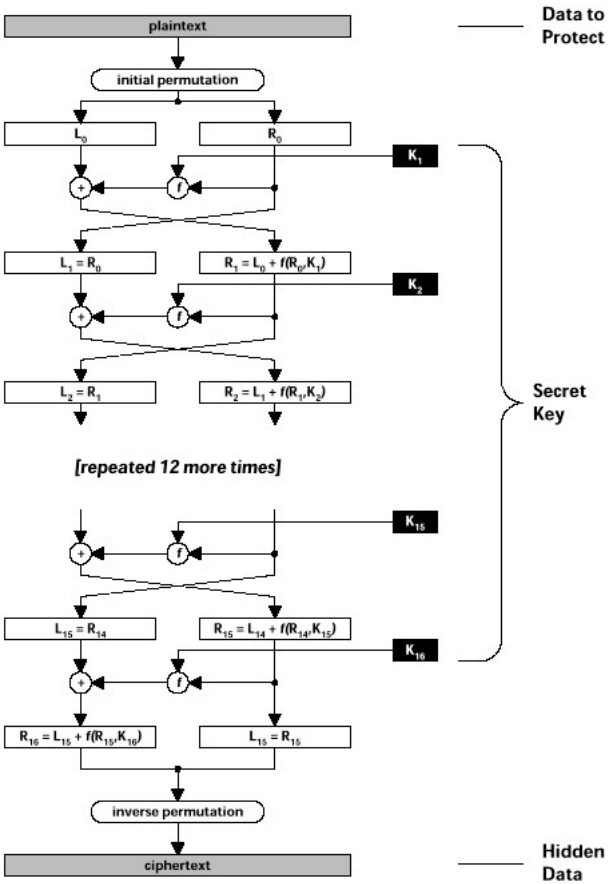
Types of Cryptography

- Hash functions
  - Compressing a message to a string of fixed length (the "message digest") such that the function is one way.
  - Popular techniques are MD4, MD5 and SHA-1



- Secret key cryptography
  - Symmetric encryption
    The same key is used for encryption and decryption
- Public key cryptography
  - Asymmetric encryption
    Separate keys for encryption and decryption,
    only one of them needs to be kept secret.

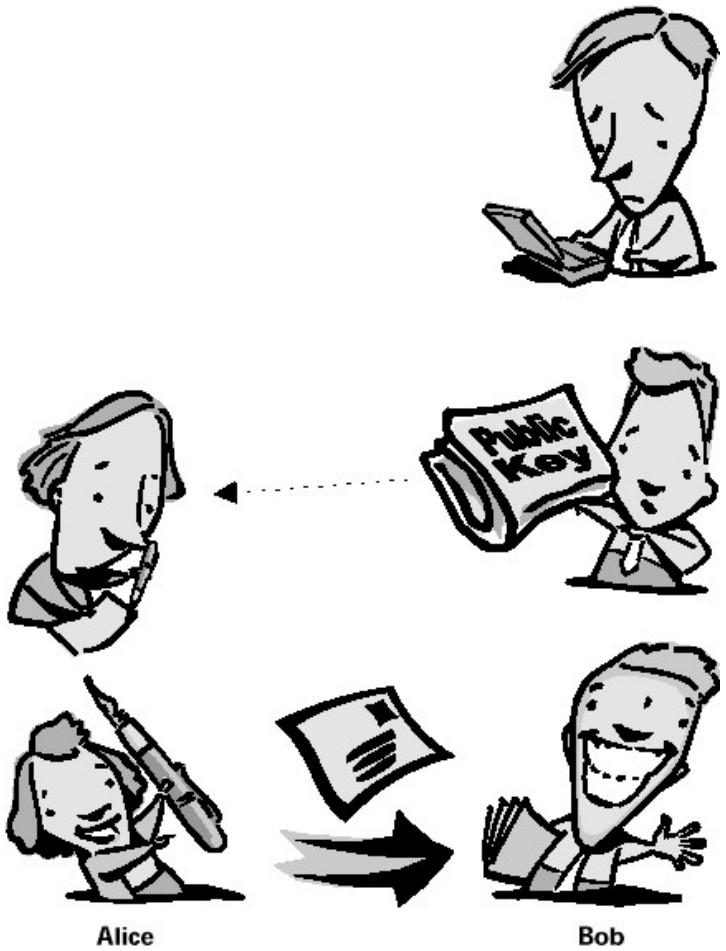
Secret key cryptography



The DES cipher

- The same key and the same mathematical transformation is used for both encryption and decryption.
- Symmetric encryption algorithms require relative small computation power and are suited for high bandwidth.
- Security is provided by reasonable keys lengths
  (at least > 64bit, usually 128-160 bit).
- Stream ciphers process byte by byte whereas block ciphers process fixed blocks of data.
- Block ciphers require an initialization vector to gain full strength.
- Common used algorithms are:
  DES, 3DES, RC2 and RC4

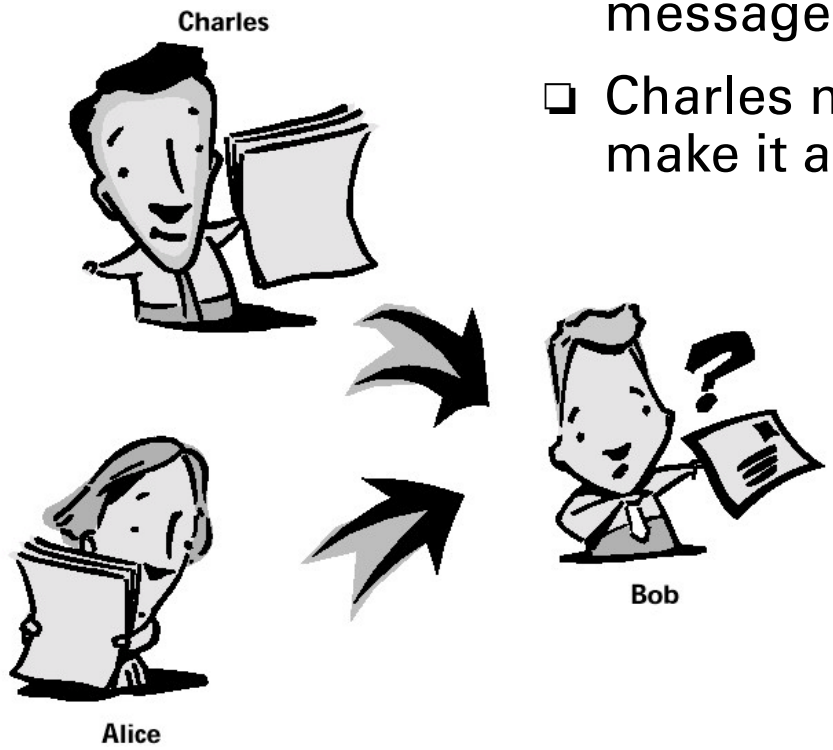
Public key cryptography



Source: Stephen Thomas; SSL and TLS Essentials

- The public key cryptography uses two different keys for encryption and decryption. Only one of the key pair needs to be kept secret (the private key), the other must not be secret at all.
- Data encrypted by the public key can only decrypted by the private key.
- Some algorithms like RSA are reversible allowing data encrypted by the private key to be decrypted by the public key.
- Public key cryptography or asymmetric encryption is very computational intensive and thus not suited for large chunks of data.

Providing Identity

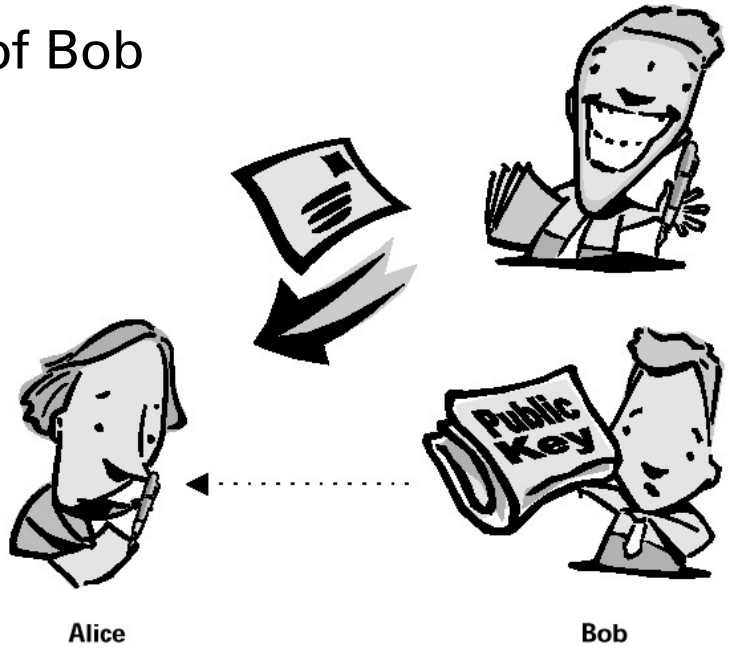


Source: Stephen Thomas; SSL and TLS Essentials

- Bob receives a message with important information, purportedly from Alice.
- How can Bob make sure that the message is really coming from Alice?
- Charles might have forged the card to make it appear as if it from Alice.

Providing identity by public key cryptography

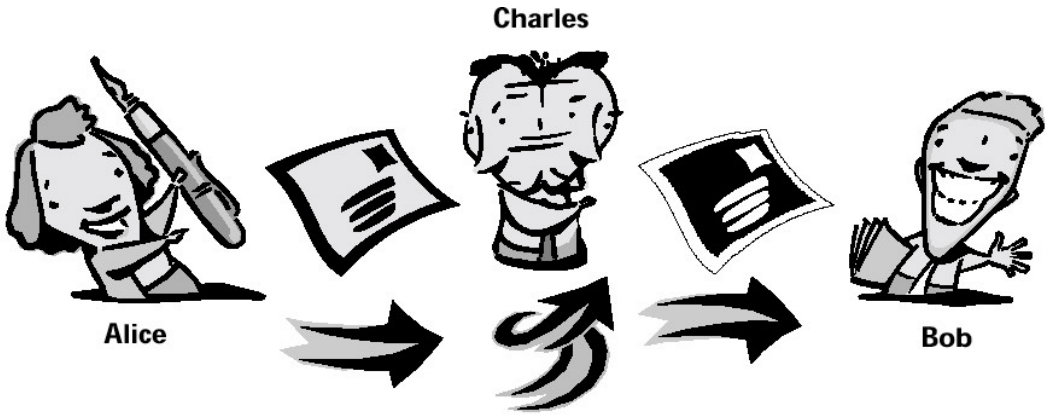
- Reversible public key algorithms such as RSA (Rivest Shamir Adleman) can be used for digital equivalent of a signature.
- Bob enciphers the message with his private key and sends the information to Alice.
- Alice can use the public key of Bob known to her to decipher the message to check whether the message is really from Bob.



Source: Stephen Thomas; SSL and TLS Essentials

Verifying information

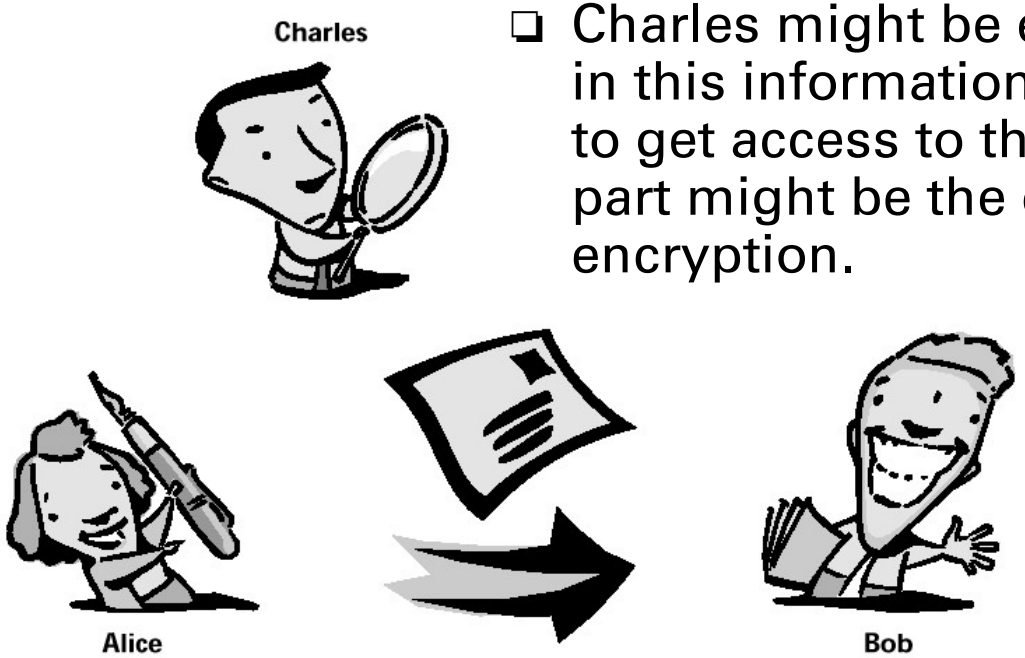
- Providing identity does not make sure the message has not altered by a man in the middle.
- Using a hash function over the whole message, generating a message digest of it and enciphering the message digest by the private key of the author provides a digital signature allowing to check the identity as well as the integrity of the message.
- The receiver decrypts the digital signature received together with the message and compares it to the message digest calculated locally.



Source: Stephen Thomas; SSL and TLS Essentials

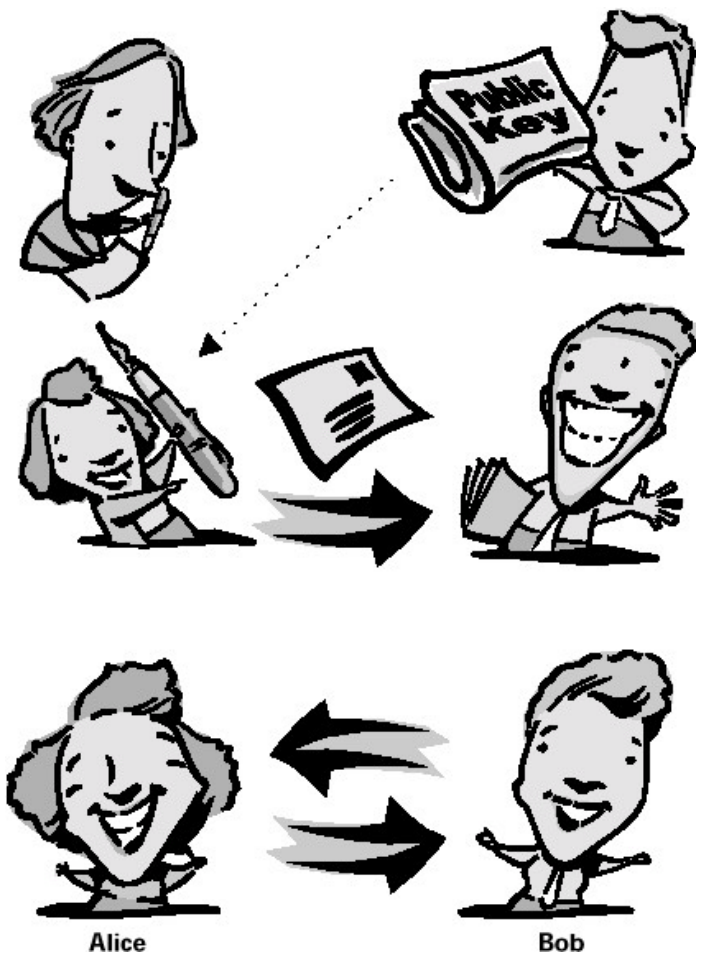
Keeping secrets

- Alice likes to send confidential information to Bob. It is extremely important, that no one other than Bob can get access to the plaintext information.
- Charles might be extremely interested in this information taking any means to get access to the data. The weakest part might be the cipher key of the encryption.



Source: Stephen Thomas; SSL and TLS Essentials

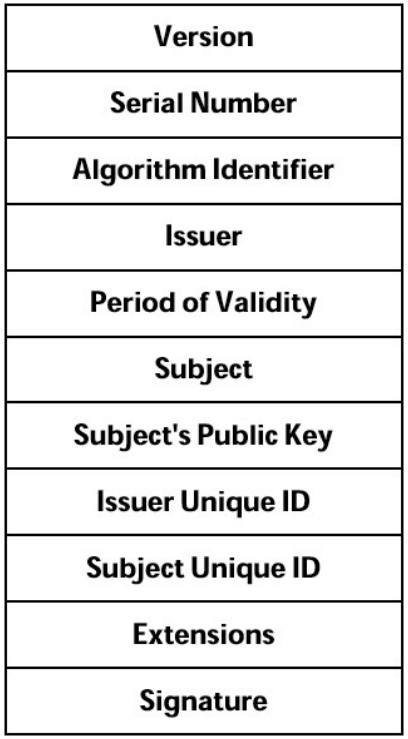
Combining secret and public key cryptography



Source: Stephen Thomas; SSL and TLS Essentials

- Keys used for symmetric encryption might be vulnerable.
- Use of public key cryptography allows to establish a new symmetric key whenever data has to be send.
- Alice generates a random number and uses the public key of Bob to encipher it and send it secret to Bob. Only Bob can decrypt the encrypted random number.
- *The Diffie-Hellman algorithm is another method to establish a secret key between two parties only using public messages.*

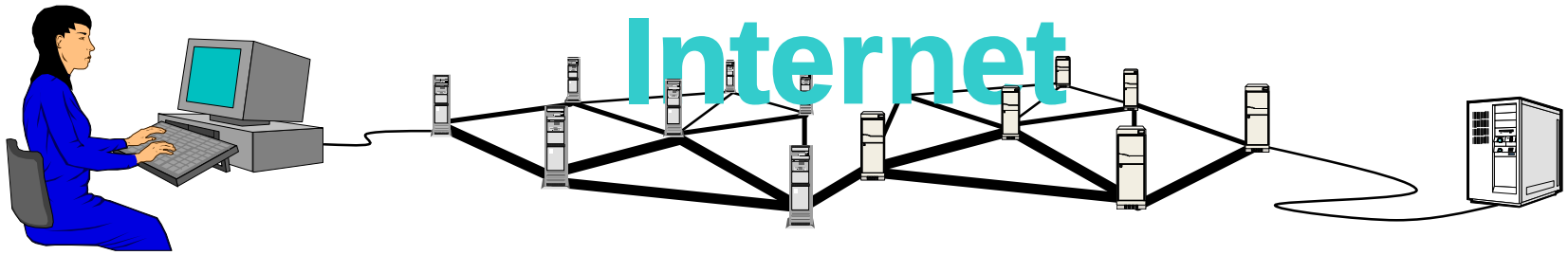
Key management



A public key certificate

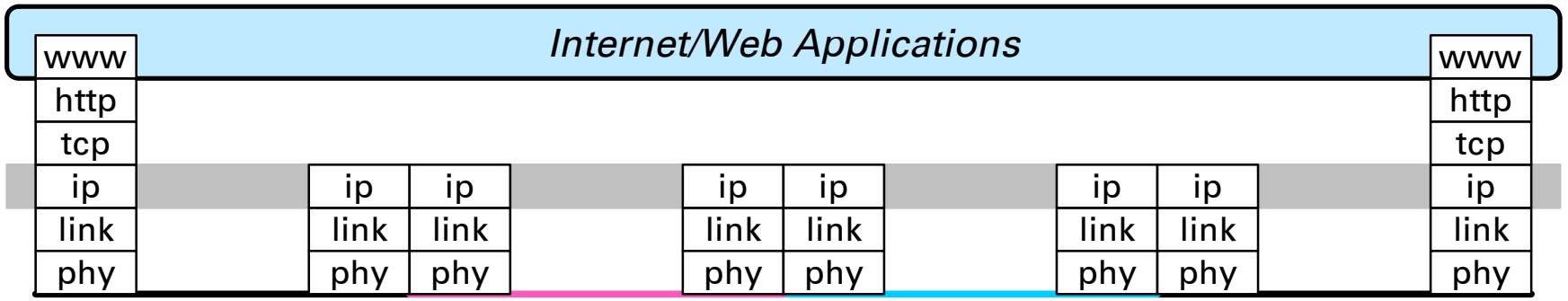
- Public key cryptography requires the reliable provisioning of the public keys. Digital signatures fully depend of the identity of the public keys.
- Public key *certificates* are electronic documents allowing the check of the validity of someone's public key.
- The public key of the Subject is signed by the private key of the Issuer. Signing means applying a hash function, generating a message digest and enciphering the message digest with the private key.
- The issuer of certificates are traditionally known as Certificate Authorities (CA).

Cryptography in the Internet



Peer
(Client)

Peer
(Server)



Cryptography can be put into any layer providing end-to-end transparency.

Security protocols