University of Massachusetts Amherst

ECE697AA – Lecture 14

Security: Cryptographic Protocols II

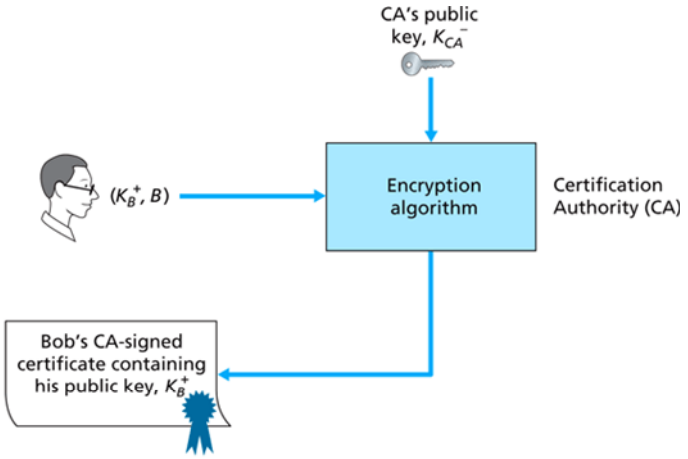
Tilman Wolf
Department of Electrical and Computer Engineering
10/23/08

Key distribution

- Symmetric key cryptography
  - A priori shared secret necessary
  - Trusted intermediary can distribute session key
    - » "Key distribution center" (KDC)
- Public key cryptography
  - Correct public key is important
    - » Man-in-the-middle attack
  - Trusted intermediary can distribute public key
    - » "Certification authority" (CA)

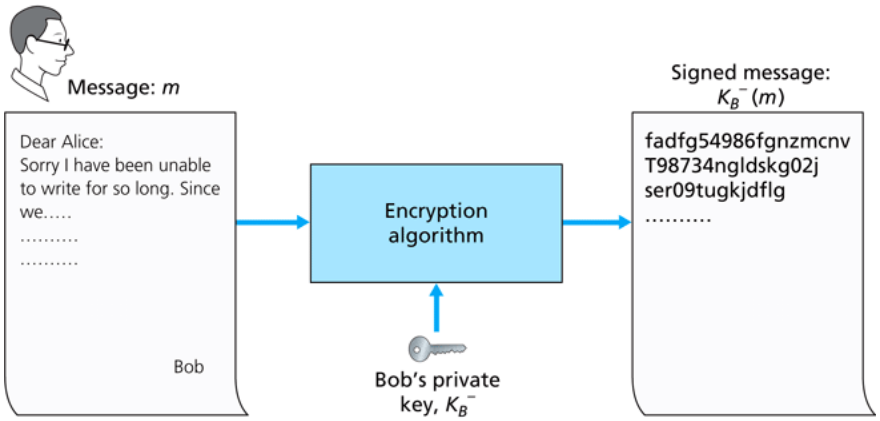
Public key certification

- Public key needs to come from trusted source
- Certificate authority can authenticate public key



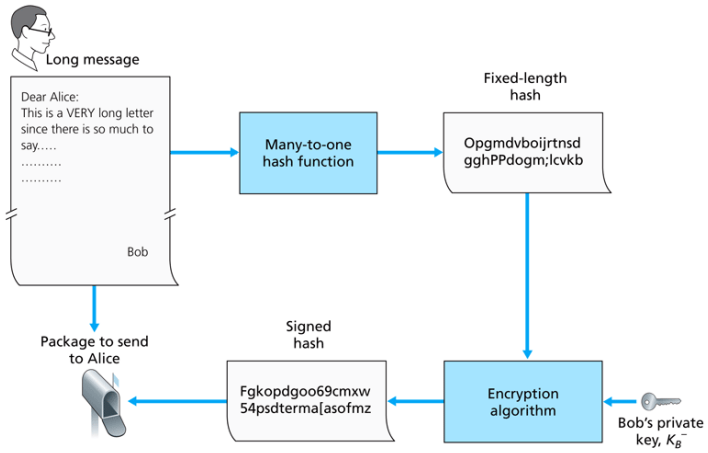
Integrity and non-repudiation

- Need signatures for documents (or keys)
  - Signatures should not be forgeable
  - Document should not be changeable after signing



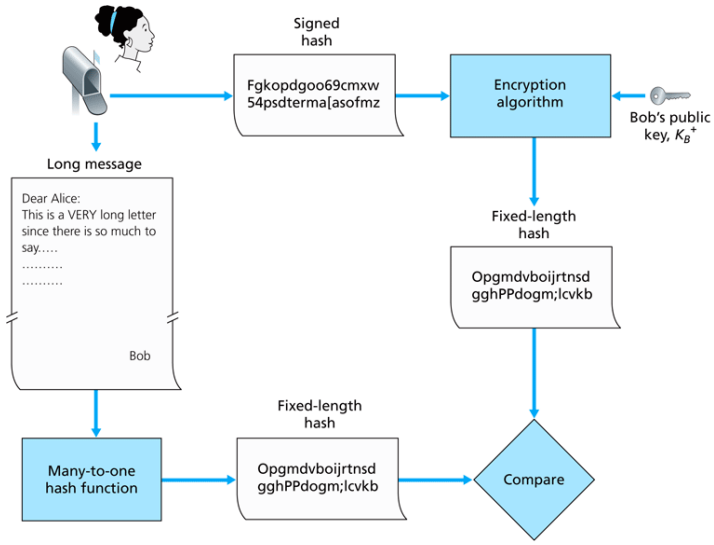
Digital signatures

- Computationally simplify signature
  - Hash of document can be used for signature
  - Cryptographic hash functions: MD5, SHA-1



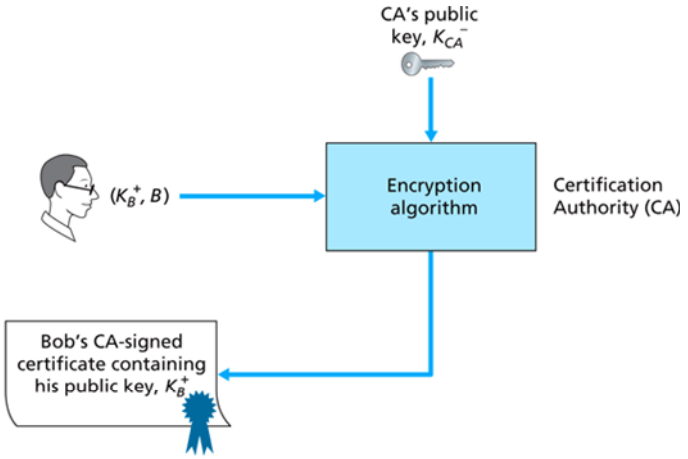
Digital signatures

- Digital signature check



Public key certification

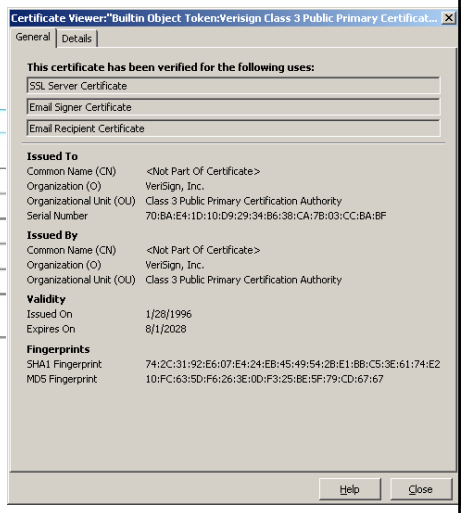
- Public key needs to come from trusted source
- Certificate authority can authenticate public key



Certificate example

- VeriSign certificate

Field Name	Description
Version	Version number of X.509 specification
Serial number	CA-issued unique identifier for a certificate
Signature	Specifies the algorithm used by CA to sign this certificate
Issuer name	Identity of CA issuing this certificate, in distinguished name (DN) [RFC 2253] format
Validity period	Start and end of period of validity for certificate
Subject name	Identity of entity whose public key is associated with this certificate, in DN format
Subject public key	The subject's public key as well as an indication of the public key algorithm (and algorithm parameters) to be used with this key



SSL certificates

http://www.verisign.com - Compare All SSL Certificates from VeriSign, Inc. - Mozilla Firefox

VeriSign

Compare All SSL Certificates

Option	Secure Site SSL Certificates	Secure Site Pro True 128-Bit SSL	Managed PKI for SSL Standard Edition	Managed PKI for SSL Premium Edition
View Product Description	Product Info	Product Info	Product Info	Product Info
Ready to Buy?	Buy Now	Buy Now	Contact Sales	Contact Sales
Price: 3-Year Certificate	$995	$2,480	Contact Sales	Contact Sales
Price: 2-Year Certificate	$695	$1,790	Contact Sales	Contact Sales
Price: 1-Year Certificate	$399	$995	$249/certificate	$695/certificate
Number of certificates	Single	Single	10 tokens or more	10 tokens or more
Free SSL Trial	Free SSL Trial	-	-	-
Minimum SSL Encryption	40-bit	128-bit	40-bit	128-bit
Issuance	Standard	Express delivery	Instant issuance by authenticated administrators	Instant issuance by authenticated administrators
VeriSign NetSure Protection Warranty	$100,000	$250,000	$100,000	$250,000

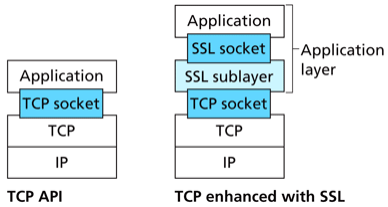
Done

Chain of trust

- Chain of trust can go multiple levels
  - Root certificates are final step
- Private keys need to protected well
- Security hardware:
  - Tamper-proof
  - On-board key generation
  - On-board cryptographic engine
  - E.g., IBM 4758 Cryptographic Coprocessor

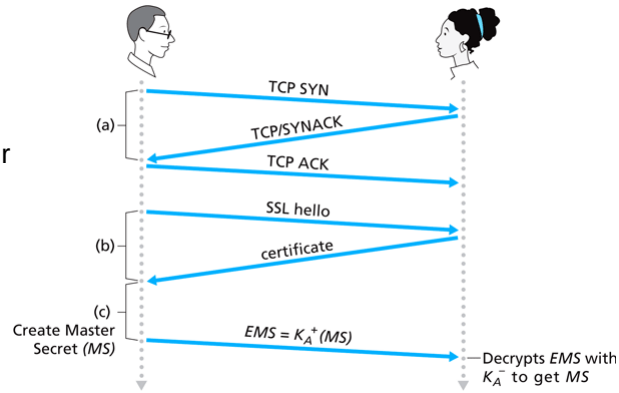
Secure network protocols

- Security in the Internet at different levels
  - Secure socket layer (SSL)
    - » Transport layer security
    - » End-to-end
    - » Usage: WWW, email, etc.
  - Secure IP (IPsec)
    - » Network layer security
    - » Subnet-to-subnet
    - » Usage: Virtual private networks (VPN)
  - Wired equivalent privacy (WEP)
    - » Link layer security
    - » Node-to-node
    - » Usage: wireless link layer



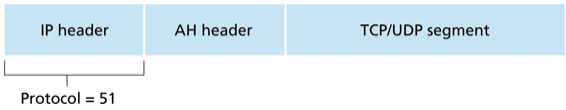
Secure Socket Layer

- SSL handshake
  - Exchange of cryptographic preferences
  - Authentication with public key cryptography
  - Exchange of symmetric session key
  - Symmetric key cryptography for data exchange



Secure IP

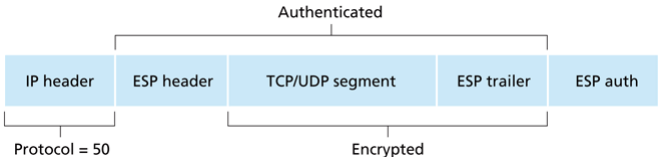
- IPsec flavors:
  - Authentication header (AH) protocol
    - » Authentication and integrity
  - Encapsulation security payload (ESP) protocol
    - » Confidentiality, authentication, and integrity
- AH header:



  - Fields: next header, security parameter index (SPI), sequence number, authentication data (digital signature)
  - HMAC (hashed message authentication code) uses shared symmetric keys

Secure IP

- ESP header:

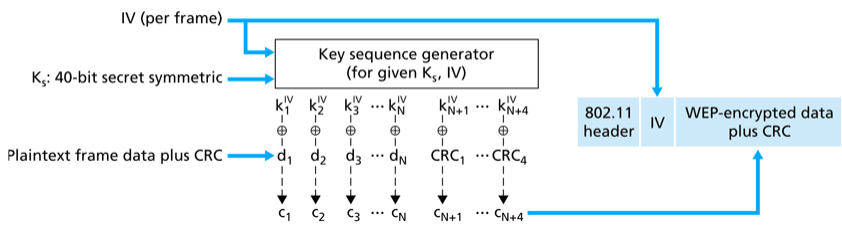


  - Authentication surrounds encrypted area
  - Key management with Internet key exchange (IKE)
  - Connection management with Internet security association and key management protocol (ISKMP)
- IPsec can be used end-to-end or in tunnel mode between routers

Wired Equivalent Privacy

- Shared symmetric key without key management
  - 40-bit key
- Authentication
  - Host request access
  - Router sends 128-bit nonce
  - Host returns encrypted nonce
  - Router decrypts nonce
- Encryption

$$c_i = d_i \oplus k_i^{IV}$$



Wired Equivalent Privacy

- Encryption is simple XOR on key
  - Initialization vector (IV) should never be reused
  - IV is plaintext in packet
  - Only 2^{24} different IVs
- Potential chosen-plaintext attack
  - Trigger transmission of known data
  - XOR reveals key values for particular IV
  - Next transmission with same IV can be decoded
- Improved security in 802.11i

Assignments

- SPARK
  - Assessment quiz
- Kurose & Ross
  - Chapter 5.1