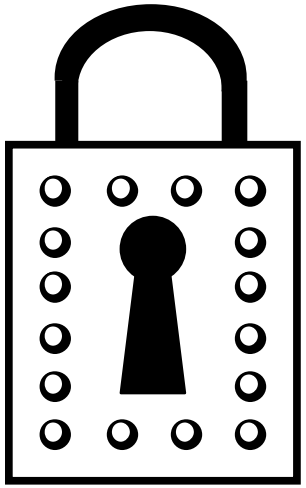
Miscellaneous Terminology



License

Commonly used names

- Some names often appear in books and articles about cryptography
- *Alice* and *Bob* are two people who want to communicate securely
- *Black hat* wants to intercept and decode or modify messages sent between Alice and Bob
- The term *black hat* comes from old cowboy movies:
  - By convention, the hero wore a white hat
  - And the villain wore a black hat
- The term *white hat* refers to somebody who fixes security loopholes in computer systems

Principal and credentials

- *Principal* is an identity
  - Think of it as being a username
- *Credentials* is the data that prove the *principal* (identity)
  - This might be a password (to go with the username) or an X509 certificate
- Human analogy:
  - “I am Dr. John Smith” (that is my *principal*)
  - “Here is my passport (or driving license)” to prove I am who I say I am (my *credentials*)
  - “Here is my license to practice medicine” to prove that I am a doctor (another set of *credentials*)

PK, PKI and IETF

- Recall:
  - *Public and private key cipher* is another name for *asymmetric cipher*
  - *Public and private key* is often abbreviated to *public key*
- *PK* is an acronym for *public key*
- *PKI* is an acronym for *public key infrastructure*
  - Supporting infrastructure required to use public keys
  - It consists of:
    - Certificate authority (CA) software
    - Procedures used verify a user's identity so the CA is willing to sign the user's certificate
- *IETF* is an acronym for the *Internet Engineering Task Force*
  - An organization that defines standards for Internet-related technologies

RSA, VeriSign and PKCS

- RSA is a public-key encryption algorithm
  - Its name is an acronym of the surnames of its inventors (Ron Rivest, Adi Shamir and Leonard Adleman)
  - It was invented in 1977 and is still widely used today
- *RSA Security* was a company set up to promote and exploit cryptographic technologies (including RSA)
  - RSA is now owned by EMC Corporation
- *PKCS* is an acronym for public *key cryptographic standards*
  - A collection of (pseudo-)standards defined by a RSA Security
  - Not officially standards, because they are defined by a company
  - However, several have been adopted by formal standards organizations
- *VeriSign* was a spin-off company from RSA Security
  - It is the largest certificate authority for the Internet

Some well-known ciphers used in SSL and TLS

- Asymmetric ciphers:
  - RSA, Diffie-Hellman, DSA, SRP, PSK
- Symmetric ciphers:
  - RC2, DES, IDEA (used only in old versions of SSL)
  - RC4, Triple DES, AES (also called Rijndael), Camellia
- Cryptographic hash functions:
  - MD2, MD4 (used only in old versions of SSL)
  - MD5, SHA-1
- An SSL *cipher suite* consists of:
  - One asymmetric cipher, plus
  - One symmetric cipher, plus
  - One cryptographic hash function

It is negotiated during the initial SSL handshaking

Some other standards

- PKCS#11 is an API used to obtain cryptographic tokens from hardware
  - For example, from a smart card
- PKCS#12 ("`.p12`") is a file format:
  - Used to store private keys with accompanying public key certificates
  - The file is encrypted for security
  - Used widely
- Privacy Enhanced MAIL (PEM)
  - An IETF proposed standard for using public key cryptography in email
  - Not widely deployed
  - PEM ("`.pem`" file extension) is used by OpenSSL
  - OpenSSL can convert between "`.pem`" and "`.p12`" file formats