Uses for Public Key Crypto

Uses for Public Key Crypto

- Confidentiality
  - Transmitting data over insecure channel
  - Secure storage on insecure media
- Authentication (later)
- Digital signature provides integrity and **non-repudiation**
  - No non-repudiation with symmetric keys

Non-non-repudiation

- Alice orders 100 shares of stock from Bob
- Alice computes **MAC** using symmetric key
- Stock drops, Alice claims she did ***not*** order
- Can Bob prove that Alice placed the order?
- **No!** Since Bob also knows the symmetric key, he could have forged message
- **Problem:** Bob knows Alice placed the order, but he can't prove it

Non-repudiation

- Alice orders 100 shares of stock from Bob
- Alice **signs** order with her private key
- Stock drops, Alice claims she did not order
- Can Bob prove that Alice placed the order?
- **Yes!** Only someone with Alice's private key could have signed the order
- This assumes Alice's private key is not stolen (revocation problem)

Public Key Notation

- **Sign** message M with Alice's **private key:** $[\mathrm{M}]_{\mathrm{Alice}}$
- **Encrypt** message M with Alice's **public key:** $\{\mathrm{M}\}_{\mathrm{Alice}}$
- Then

$$\{[\mathrm{M}]_{\mathrm{Alice}}\}_{\mathrm{Alice}} = \mathrm{M}$$

$$[\{\mathrm{M}\}_{\mathrm{Alice}}]_{\mathrm{Alice}} = \mathrm{M}$$

Public Key Infrastructure

Public Key Certificate

- **Certificate** contains name of user and user's public key (and possibly other info)
- It is ***signed*** by the issuer, a ***Certificate Authority*** (CA), such as VeriSign

  M = (Alice, Alice's public key), $\mathrm{S} = [\mathrm{M}]_{\mathrm{CA}}$

  Alice's Certificate = (M, S)
- Signature on certificate is verified using CA's public key:

  Verify that $\mathrm{M} = \{\mathrm{S}\}_{\mathrm{CA}}$

Certificate Authority

- Certificate authority (CA) is a trusted 3rd party (TTP) — creates and signs certificates
- Verify signature to verify integrity & identity of **owner of corresponding private key**
  - Does **not** verify the identity of the **sender** of certificate — certificates are public keys!
- Big problem if CA makes a mistake (a CA once issued Microsoft certificate to someone else)
- A common format for certificates is X.509

PKI

- Public Key Infrastructure (PKI): the stuff needed to securely use public key crypto
  - Key generation and management
  - Certificate authority (CA) or authorities
  - Certificate revocation lists (CRLs), etc.
- No general standard for PKI
- We mention 3 generic “trust models”

PKI Trust Models

- Monopoly model
  - One universally trusted organization is the CA for the known universe
  - Big problems if CA is ever compromised
  - Who will act as CA???
    - System is useless if you don't trust the CA!

PKI Trust Models

- Oligarchy
  - Multiple trusted CAs
  - This is approach used in browsers today
  - Browser may have 80 or more certificates, just to verify certificates!
  - User can decide which CAs to trust

PKI Trust Models

- Anarchy model
  - Everyone is a CA…
  - Users must decide who to trust
  - This approach used in PGP: "Web of trust"
- Why is it anarchy?
  - Suppose a certificate is signed by Frank and you don't know Frank, but you do trust Bob and Bob says Alice is trustworthy and Alice vouches for Frank. Should you accept the certificate?
- **Many** other trust models and PKI issues

Confidentiality in the Real World

Symmetric Key vs Public Key

- Symmetric key +'s
  - **Speed**
  - No public key infrastructure (PKI) needed
- Public Key +'s
  - **Signatures** (non-repudiation)
  - No ***shared*** secret (but, private keys…)

Notation Reminder

- Public key notation
  - Sign M with Alice's **private key**

    $[\mathrm{M}]_{\mathrm{Alice}}$
  - Encrypt M with Alice's **public key**

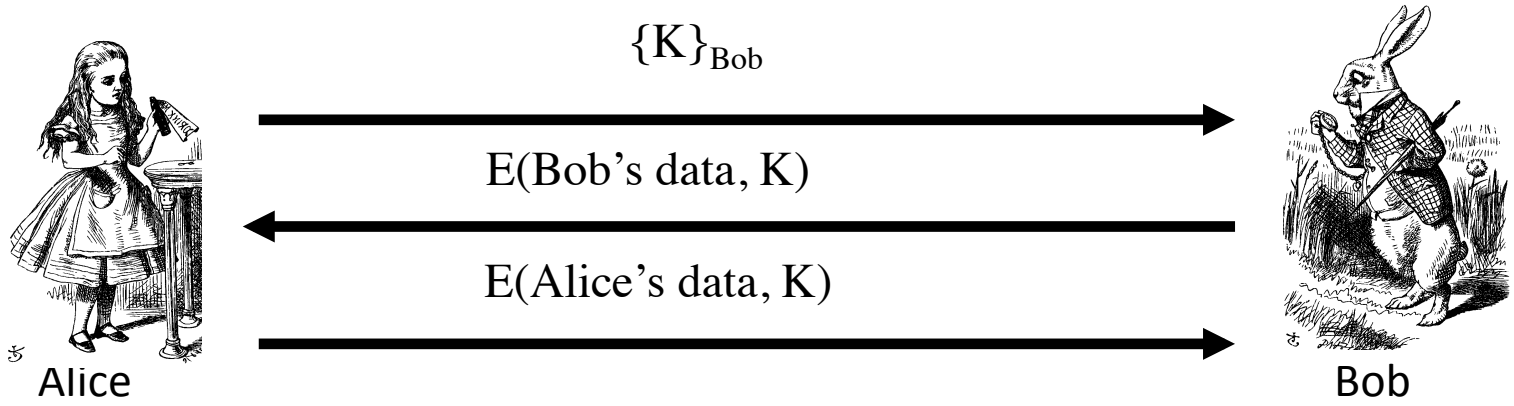
    $\{\mathrm{M}\}_{\mathrm{Alice}}$
- Symmetric key notation
  - Encrypt P with symmetric key K

    $\mathrm{C} = \mathrm{E}(\mathrm{P},\mathrm{K})$
  - Decrypt C with symmetric key K

    $\mathrm{P} = \mathrm{D}(\mathrm{C},\mathrm{K})$

Real World Confidentiality

- **Hybrid cryptosystem**
  - Public key crypto to establish a key
  - Symmetric key crypto to encrypt data…



- Can Bob be sure he's talking to Alice?