University of Massachusetts Amherst

# ECE697AA – Lecture 13

Security: Cryptographic Protocols

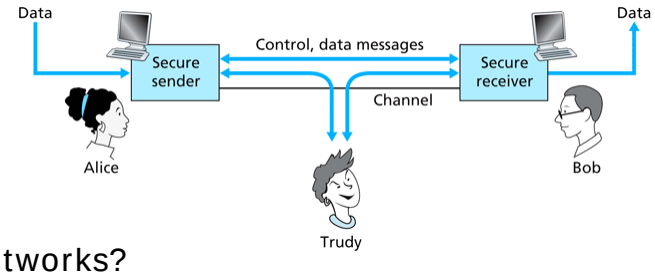
Tilman Wolf
Department of Electrical and Computer Engineering
10/17/08

## Secure communication

- What are the properties of secure communication?
- Confidentiality
  - Content is hidden
- Authentication
  - Source is verified
- Message integrity and non-repudiation
  - Message is unchanged and undeniable
- Availability and access control
  - Legitimate users should have access
- Examples in the Internet?

# Attack models

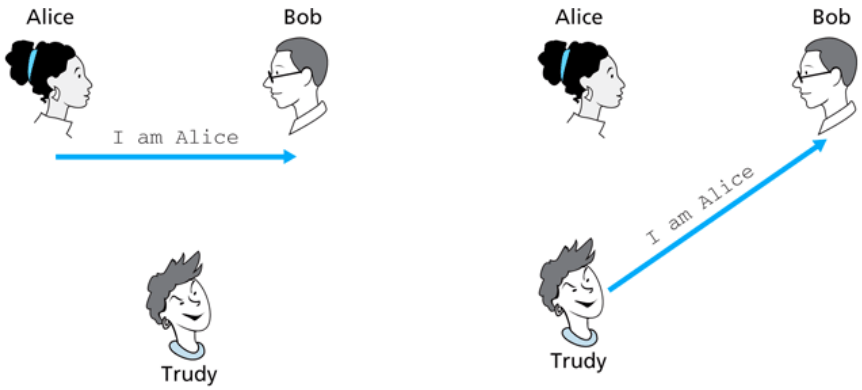
- Attacker can
  - Eavesdrop
  - Modify
  - Insert
  - Delete
- How can that be done in networks?
  - Wireless link
  - Modify DNS
  - Corrupt routing computation
  - Other network management functions
- How can we provide security?
  - Simplest case: authentication





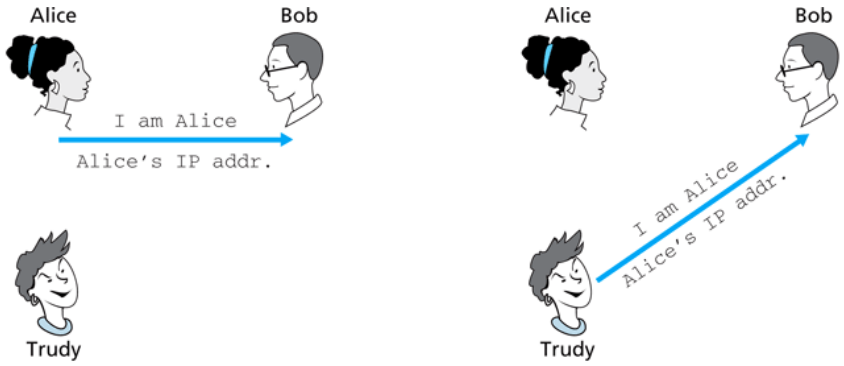

# Authentication protocol

- Authentication identifies “other side” of communication



# Authentication protocol

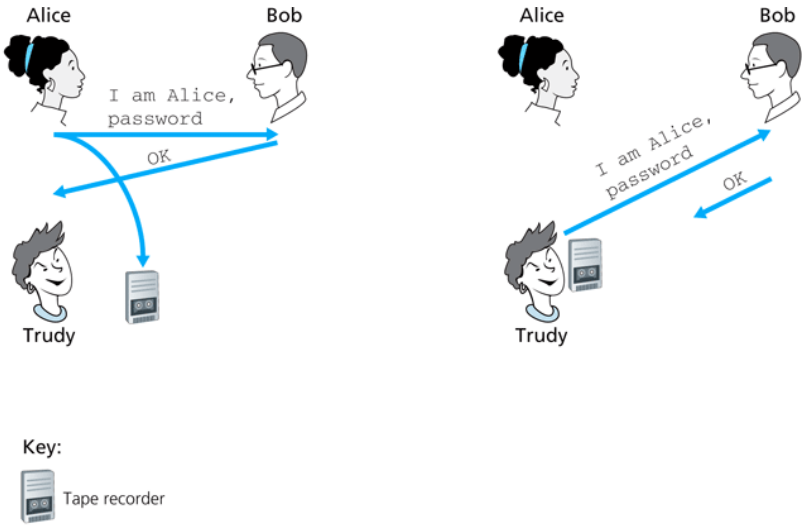
- Authentication by network identifier does not help





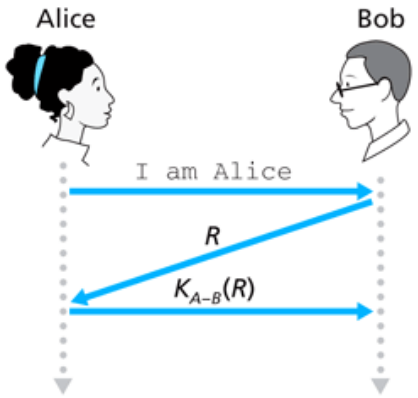

# Authentication protocol

- Password does not help against replay attacks



# Authentication protocol

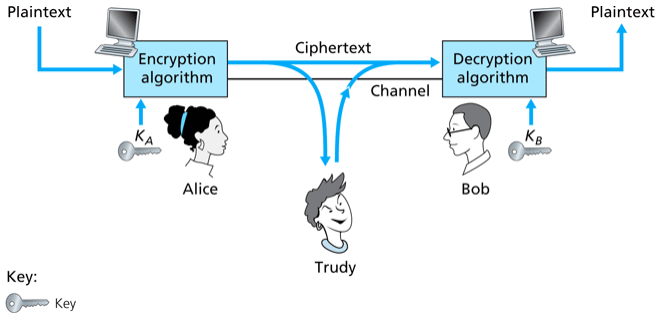
- Replay attacks can be foiled by use of “nonce”
  - Random number chosen by receiver






# Cryptographic principles

- Standard cryptographic scenario




- Algorithm should be key-based
  - Security through obscurity does not work
  - Kerckhoff's principle:
    - » All algorithms must be public; only the keys are secret

# Symmetric key cryptography

- Monoalphabetic cipher

| | |
|---|---|
| Plaintext letter: | a b c d e f g h i j k l m n o p q r s t u v w x y z |
| Ciphertext letter: | m n b v c x z a s d f g h j k l p o i u y t r e w q |

- Potential attacks
  - Ciphertext-only attack
  - Known-plaintext attack
  - Chose-plaintext attack
- More secure:
  - Polyalphabetic cipher

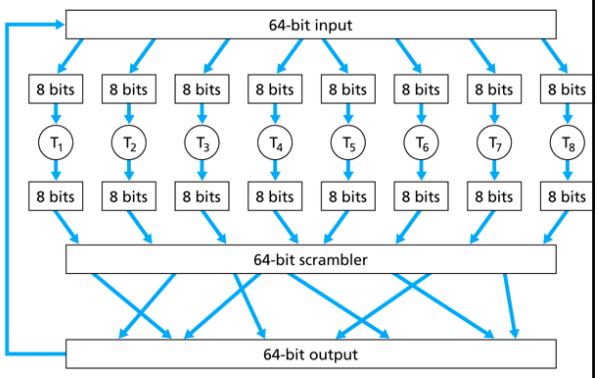
| | |
|---|---|
| Plaintext letter: | a b c d e f g h i j k l m n o p q r s t u v w x y z |
| $C_1(k = 5)$: | f g h i j k l m n o p q r s t u v w x y z a b c d e |
| $C_2(k = 19)$: | t u v w x y z a b c d e f g h i j k l m n o p q r s |

  - Lots of other encryption algorithms



# Block cipher

- Goal
  - Ever bit of ciphertext depends on every bit of cleartext and key
  - Scramble data into pseudo-random sequence
- Examples:
  - Data Encyption Standard (DES)
    - » 64-bit block with 56-bit key
  - 3DES
  - Advanced Encryption Standard (AES)
    - » 128-bit block with 128, 192, or 256-bit key
- Symmetry of algorithm
  - Same process for encryption and decryption



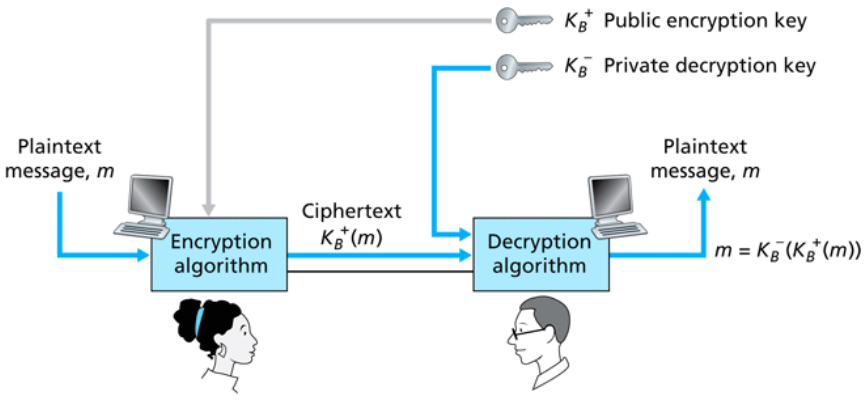
# Data Encryption Standard

- Cracking DES:
  - Exhaustive search
  - Jan 97: four months
  - Feb 98: 41 days
  - Jan 99: 22 hours (checked 245 billion keys/sec)
- More secure version:
  - Triple-DES (3DES)
    - » Use three keys
    - » Output from first DES step is input to second, …
  - Cipher-block chaining:
    - » Cleartext block is XORed with encrypted previous block



# Public key encryption

- Asymmetric encryption
  - Different keys for encryption and decryption
- RSA (Rivest, Shamir, Adleman) algorithm



# Public key encryption

- Choice of keys:
  - Choose two prime numbers $p$ and $q$
  - Compute $n = pq$ and $z = (p-1)(q-1)$
  - Choose $e < n$, such that it has no common factors with $z$
  - Find $d$, such that $ed-1$ is divisible by $z$
- Usage:
  - Public key: $(n,e)$
  - Private key: $(n,d)$
  - Encryption: $c = m^e \bmod n$
  - Decryption: $m = c^d \bmod n$



# Public key Encryption

- Toy example:
  - Choose $p=5$ and $q=7$
    - » Thus, $n=35$ and $z=24$
  - Choose $e=5$, since 5 and 24 have no common factors
  - Choose $d=29$, since $5 \cdot 29-1$ is divisible by 24
  - Public key: (35, 5)
  - Private key: (35, 29)

# Public key encryption

- Encryption:

| Plaintext Letter | $m$: numeric representation | $m^e$ | Ciphertext $c = m^e \bmod n$ |
|---|---|---|---|
| l | 12 | 248832 | 17 |
| o | 15 | 759375 | 15 |
| v | 22 | 5153632 | 22 |
| e | 5 | 3125 | 10 |

- Decryption:

| Ciphertext $c$ | $c^d$ | $m = c^d \bmod n$ | Plaintext Letter |
|---|---|---|---|
| 17 | 481968572106750915091509141182522307169 7 | 12 | l |
| 15 | 127834039403948858939111232757568359375 | 15 | o |
| 22 | 851643319086537701956194499721106030592 | 22 | v |
| 10 | 10000000000000000000000000000000 | 5 | e |

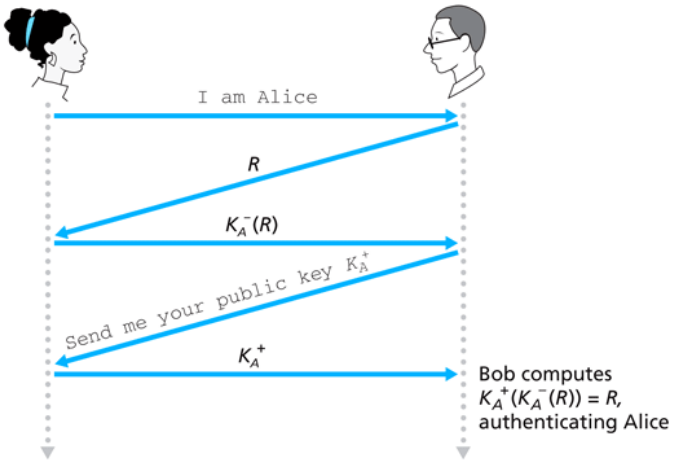


# Public key encryption

- "Magic" in RSA
  - $(m^e)^d \bmod n = m^{ed} \bmod n$
  - From number theory
    - » If $p$, $q$ prime and $n=pq$, then $xy \bmod n = x^{(y \bmod (p-1)(q-1))} \bmod n$
  - $(m^e)^d \bmod n = m^{(ed \bmod (p-1)(q-1))} \bmod n$
  - $e$, $d$ chosen such that $ed$-1 is divisible by $(p-1)(q-1)$
    - » Thus, $ed \bmod (p-1)(q-1) = 1$
  - $(m^e)^d \bmod n = m^1 \bmod n = m$
  - Same for $(m^d)^e = (m^d)^e = m^{ed}$
- Public key encryption has broad range of application
  - Confidentiality
  - Authentication
  - Integrity and non-repudiation

# Authentication protocol

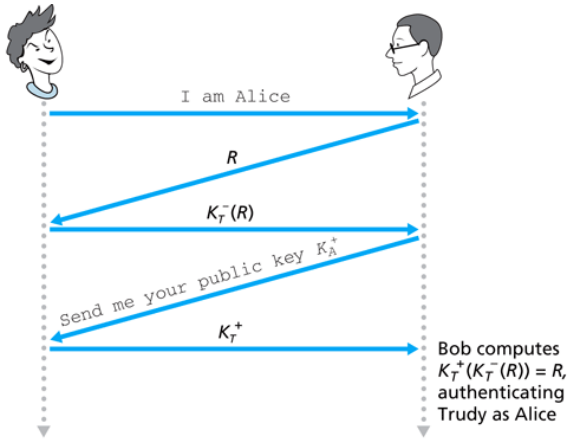
- Can also be used with asymmetric keys





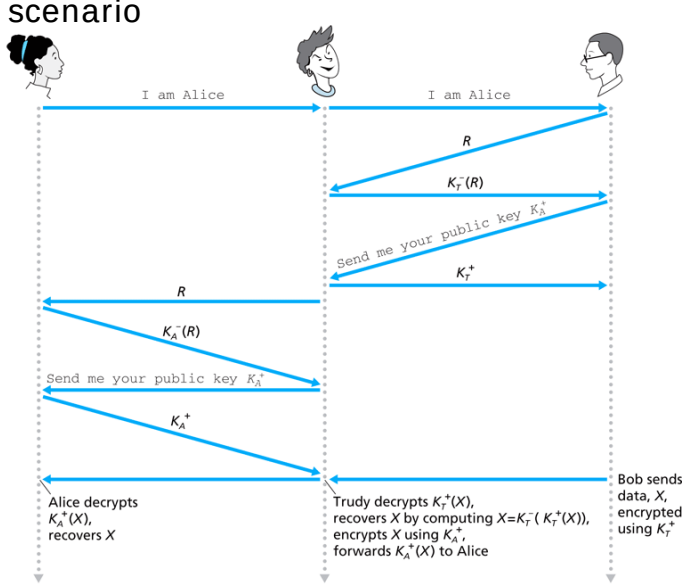

# Authentication protocol

- Attacker can pose as other side
  - Receiving public key on the same channel as encoded nonce is bad idea



# Man-in-the-middle attack

- Classic scenario






# Man-in-the-middle attack

- How can we avoid a man-in-the-middle attack?

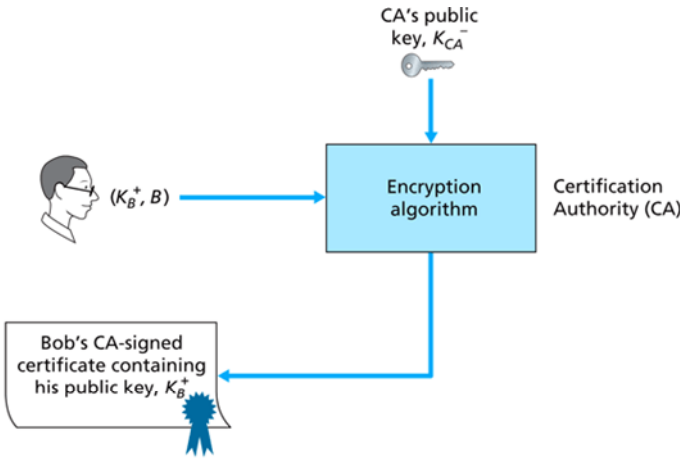
# Key distribution

- 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

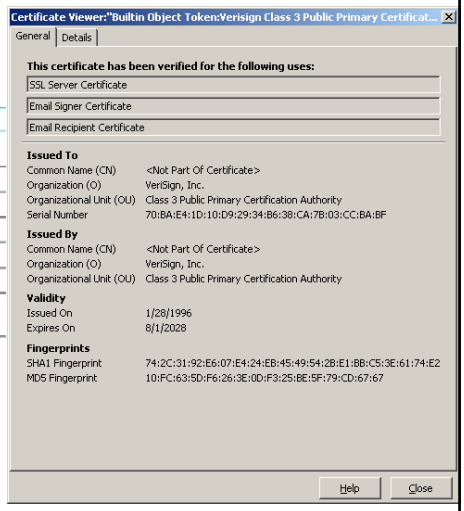
- Public key needs to come from trusted source
- Certificate authority can authenticate public key



# 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 |






# Assignments

- SPARK
  - Assessment quiz