Computer and Network Security

Lecture 3

Symmetric – Asymmetric Cryptography

Administrative

- Slides are online
  - http://lsd.ls.fi.upm.es/lsd/education
- Questions?
  - csoriente@fi.upm.es

Outline

- Conventional Cryptography
- Public-key Cryptography

Cryptosystems
(at least) 5 ingredients

- Key (secret)
  - **k** ∈ ***K***
- Plaintext (cleartext)
  - Message **m** ∈ ***M***
- Ciphertext
  - Message **c** ∈ ***C***
- Encryption
  - Algorithm ***E: K x M → C***
- Decryption
  - Algorithm ***D: K x C → M***

Security should only depend on the secrecy of the keys!!!

(some) Cryptoattacks

- Ciphertext-only attack
  – Eve only sees ciphertexts
- Known plaintext attack
  – Eve sees pairs [plaintext-ciphertext]
- Chosen plaintext attack
  – Eve picks plaintexts to be encrypted
- Chosen ciphertext attack
  – Eve picks ciphertexts to be decrypted

- Bruteforce attack
  – Try all possible keys

Types of attainable security

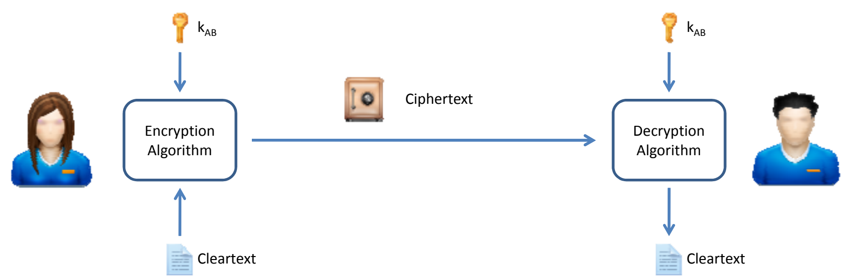
- Perfect, unconditional or information-theoretic:
  – security is evident free of any assumptions

- Provable:
  – security can be shown to be based on some common (often unproven) assumptions
    - Discrete logarithm problem
      – Given p prime and $Z_p^*=\{1,\ldots,p-1\}$
      – Find x s.t. $a^x = b \mod p$

- Ad hoc:
  – the security seems good…

Conventional (symmetric) Cryptography

- Alice and Bob share a key k_{AB} which they somehow agree upon (how?)
  - Examples: Substitution, Vernam OTP, DES, AES



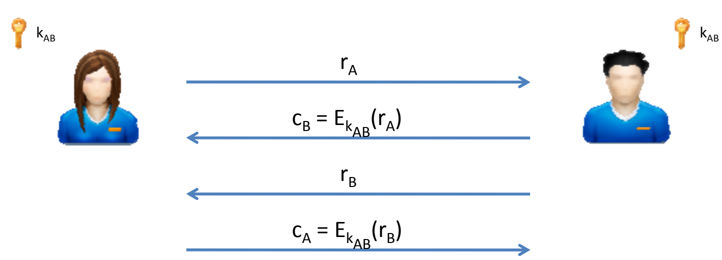
Notation

- Cleartext / Message — m
- Ciphertext — c
- Secret key — k
  - Secret key of A — k_A
- Encryption of m using k_A — $c = E_{k_A}(m)$
- Decryption of c using k_A — $m = D_{k_A}(c)$

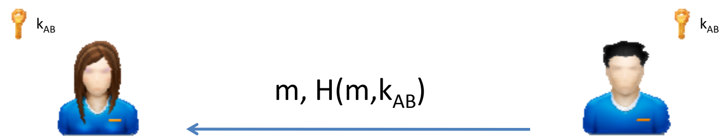
Applications of Conventional Cryptography

- Secure transmission (confidentiality)
  - Communication over insecure channels
- Secure storage (one party?)
  - char *crypt(const char **key*, const char **salt*);
- Strong authentication
  - proving knowledge of a secret without revealing it
- Integrity check
  - fixed-length checksum for message via secret key cryptography

Challenge-Response Authentication



Integrity check

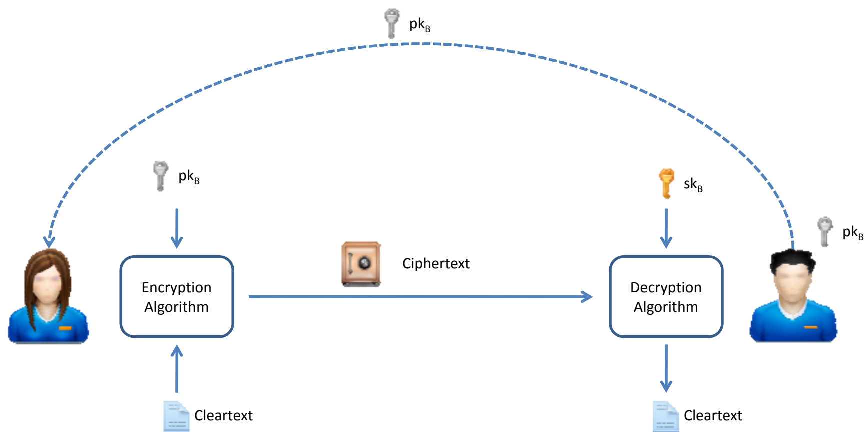


Conventional Cryptography

- Advantages
  - High data throughput
  - Relatively short key size
  - Primitives to construct various cryptographic mechanisms
- Disadvantages
  - Key must remain secret at both ends
  - Key must be distributed securely and efficiently
  - Relatively short key lifetime

Public-key (asymmetric) Cryptography

- Bob has a public/private key pair (pk_B, sk_B)
  - Examples: RSA, El Gamal



Notation

- Cleartext / Message — m
- Ciphertext — c
- Secret key — sk
  - Secret key of A — sk_A
- Public key — pk
  - Public key of A — pk_A
- Encryption of m using k_A — $c = E_{pk_A}(m)$
- Decryption of c using k_A — $m = D_{sk_A}(c)$

Applications of Public-key Cryptography

- Secure transmission (confidentiality)
  - Alice encrypts using pk_B
  - Bob decrypts using sk_B
- Secure Storage
  - encrypt with own public key
  - later decrypt with own private key
- Digital Signatures
  - authentication, integrity, non-repudiation, …

Public-key Cryptography

- Advantages
  - only the private key must be kept secret
  - relatively long life time of the key
  - more security services
- Disadvantages
  - low data throughput
  - much larger key sizes
  - distribution/revocation of public keys
  - security "provable"
    - based on conjectured hardness of certain computational problems

Comparison

- Services
  - Conventional
    - encryption and some data integrity applications
  - Public key
    - encryption, signatures, …
- Key sizes
  - Conventional
    - E.g., 64 bits for DES64 or 128 bits for AES
  - Public-key
    - 1024 bits for RSA
- Most attacks on “good” conventional cryptosystems are exhaustive key search (brute force)
- Public key cryptosystems are subject to “short-cut” attacks (e.g., factoring large numbers in RSA)