

Security and Cryptosystems

Arvind Swaminathan

Topics

- Network Attacks
- Symmetric Ciphers
- Public-Key Cryptosystems
- PGP, PEM

Introduction

- Postal mail:
 - messages are private
 - messages can be signed

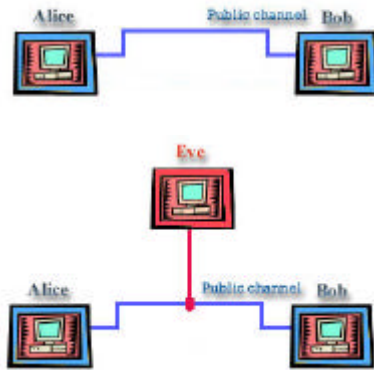


Cryptography

- Privacy: message is available to only the sender and recipient – concealed from others.
- Verify that message is from the “right person”.



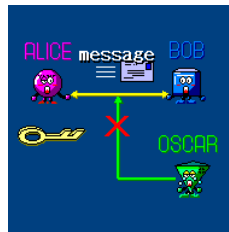
Privacy



Two “friends”
communicating over a
channel.

Eve trying to snoop,
analyze ...

Privacy



Eve\Oscar only hear garbled message

Signatures



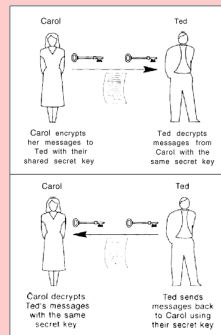
“Man in the middle” problem



Cryptosystems

- Symmetric Ciphers (secret-key cryptosystem)
 - One-time pads, DES, AES, Blowfish, IDEA, RC4
- Public-key cryptosystems
 - RSA, Diffie-Hellman, Rabin, LUC, XTR, El Gamal
- Hash Functions
 - MD5, SHA

Symmetric Ciphers



Symmetric Ciphers

- “Traditional cryptography is based on the sender and receiver of a message knowing and using the same secret key: the sender uses the secret key to encrypt the message, and the receiver uses the same secret key to decrypt the message.” — *Joseph M. Reagle, W3C.*

Symmetric Ciphers

- Vernam's one-time pad is an example of symmetric encryption, in which the same key is used to both encode and decode a message.
- Many of the encryption schemes available today are also symmetric. E.g., the DES.
- The DES is a block cipher.

Symmetric Ciphers

- Block cipher
 - It encodes text in fixed-bit blocks using a key whose length is also fixed in length.
- Stream cipher
 - It encodes the stream of data sequentially without segmenting it into blocks.

DES

- The Data Encryption Standard (DES) uses a bit-scrambling algorithm F . ($F \rightarrow$ *Fiestel algorithm*)
- It relies on exclusive-or: $A \text{ XOR } B = C$;
 $C \text{ XOR } B = A$
- Start with a 56-bit shared-secret key K
- Rotate and permute bits to generate 16 other keys K_1, K_2, \dots, K_{16}

DES

- Take 64 bits (56 + 8 parity) of message text M and permute the bits into P_0
- Split into left and right 32-bit halves L_0 and R_0
- Apply 16 rounds of a bit-scrambling algorithm
- Combine L_{16} and R_{16} into the 64-bit P_{16}

DES

- Apply a final permutation to P_{16} generate the cipher C
- Receiver gets C and knows K and so generates $K_0 \dots K_{16}$
- From C regenerate P_{16}
- The bit-scrambling algorithm is reversible for decryption

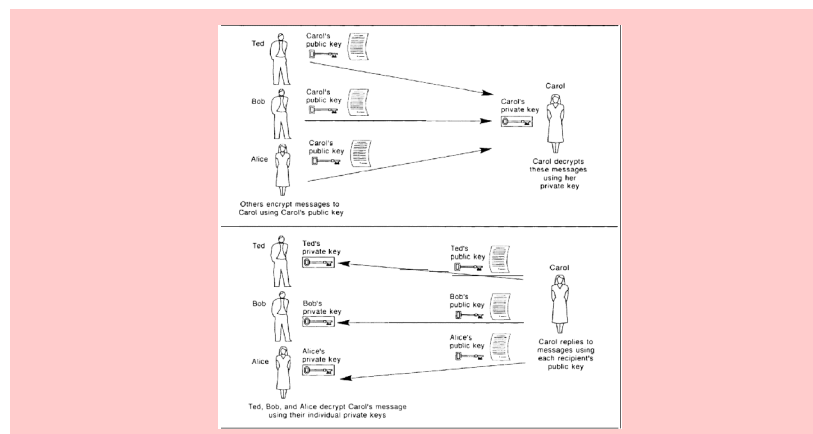
DES

- Apply K_{16} to get $P_{15} \dots P_0$ and finally M
- For longer messages, we cannot use K repeatedly.
- Advantages:
 - Simplicity

DES

- Advantages
 - The single key must be transferred from the sender to the receiver securely. If there is a secure means of transferring the key, then there may also be a secure means of transferring the message, thus encryption may not be necessary.
 - The key cannot (or should not) be reused.

Public-key Cryptosystems



Public-key Cryptosystems

- **Public Key Protocol**

- Public key transformation is one way encryption with a secret way to decrypt.
- Each user has two keys - a public key and a private key.
- Each user's public key is listed in a public directory much like a phone book.
- Each user must carefully guard against disclosing his/her private key.

US Military Crypto Basics Lectures

PKC and private encryption



- Advantage

- The message is private, since no one but Alice can decrypt the message

PKC and private encryption

- Disadvantage



Alice cannot be sure that Bob is really the sender of the message, since only her key was used to encrypt the message. Indeed, since Alice's public key is accessible to all, anyone could have encrypted the message and then sent it to Alice claiming to be Bob.

Trapdoor

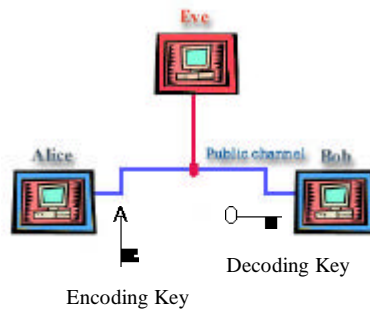
- Public Key Cryptography (PKC) is based on the idea of a “trapdoor” function

$$f: X \rightarrow Y$$


i.e.,

- f is one-to-one
- f is easy to compute
- f is public
- f^{-1} is difficult to compute
- f^{-1} becomes easy to compute if a trapdoor is known

The RSA Cryptosystem

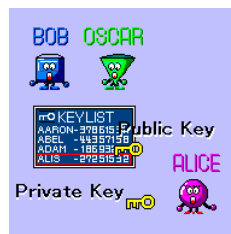


The RSA Cryptosystem

- In DES, the encoding and decoding keys are the same and must be made known to both parties before communications will work.
- In 2-key systems, the encoding and decoding keys are different. 
- A message encrypted with the encoding key can only be decrypted with the decoding key.

The RSA Cryptosystem

- In a two-way 2-key system, the reverse is also true:
 - a message *encrypted* with the decoding key can only be *decrypted* with the encoding key.



Of the pair, keep one key secret but make the other publicly available.

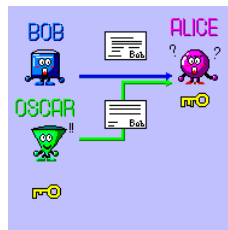
The RSA Cryptosystem

- Choose two (large) prime numbers: p, q and calculate $n = p \cdot q$
- Then define the two keys d and e
 - $C = M^e \pmod{n}$; and $M = C^d \pmod{n}$;
- Using the Chinese Remainder Theorem, this has a solution iff:
 - $e \cdot d = 1 \pmod{\tilde{a}(n)}$ where $\tilde{a}(n) = \text{lcm}(p-1, q-1)$

The RSA Cryptosystem

- Pick one of e or d and use the knowledge of the values of p and q to calculate the other using the extended Euclidean algorithm.

The Key Management Problem



- Key Distribution Centers
- Certificate Authorities

Pretty Good Privacy

- Collect public keys of people you know **in person**
- Get people to sign certificates for your public key
- Collect certificates signed by people you know **and trust**

Privacy-Enhanced Mail

- A has S_A ; publishes P_A with CA_A
- A gets P_B and chain to CA_B
- A chooses per-message DES key K
- A sends:
 - P_A + certificate-chain for CA_A
 - Initial vector for DES CBC
 - $P_B(K)$
 - $K(M+S_A(\text{MD5}(M)))$ to B