Private-Key Management and the Public-Key Revolution

Yu Zhang

HIT/CST/NIS

Cryptography, Spring, 2012

Outline

1. Limitations of Private-Key Cryptography
2. The Public-Key Revolution
3. Diffie-Hellman Key Exchange

Content

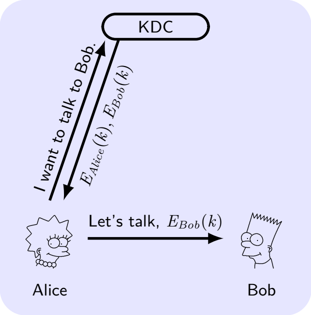
Limitations of Private-Key Cryptography

- The key-distribution need physically meeting.
- The number of keys for U users is $\Theta(U^2)$.
- Secure communication in open system:

Solutions that are based on private-key cryptography are not sufficient to deal with the problem of secure communication in open systems where parties cannot physically meet, or where parties have transient interactions.

Needham-Schroeder Protocol

- Key Distribution Center (KDC) as Trusted Third Party (TTP).
- $E_{Bob}(k)$ is a **ticket** to access Bob, k is **session key**.
- Used in MIT's Kerberos protocol (in Windows).



Strength:

- each one stores one key.
- no updates.

Weakness:

- all-or-nothing.
- single-point-of-failure.

Merkle Puzzles (Key Exchange W/O TTP)

Alice prepares 2^{32} puzzles Puzzle_i, and sends to Bob.

$$\mathsf{Puzzle}_i \leftarrow \mathsf{Enc}_{(0^{96}\|p_i)}(\text{“Puzzle \#”}x_i\|k_i),$$

where Enc is 128-bit, $p_i \leftarrow \{0,1\}^{32}$ and $x_i, k_i \leftarrow \{0,1\}^{128}$.

Bob chooses Puzzle_j randomly, guesses p_j in 2^{32} time, obtains x_j, k_j and sends x_j to Alice.

Alice lookups puzzle with x_j, and uses k_j as secret key.

- **Adversary** needs 2^{32+32} time.

Better Gap?

Quadratic gap is best possible if we treat cipher as a black box oracle.

Content

Public-Key Revolution

- In 1976, Whitfield Diffie and Martin Hellman published "*New Directions in Cryptography*".
- **Asymmetric** or **public-key** encryption schemes:
  - **Public key** as the encryption key.
  - **Private key** as the decryption key.
- **Public-key primitives**:
  - Public-key encryption.
  - Digital signatures. (non-repudiation)
  - Interactive key exchange.
- **Strength**:
  - Key distribution over public channels.
  - Reduce the need to store many keys.
  - Enable security in open system.
- **Weakness**: slow, active attack on public key distribution.
- **Peoples**: Ralphe Merkle (his advisor at Stanford was Hellman), Michael Rabin, Rivest, Shamir, and Adleman.

Content

The Setting and Definition of Security

The key-exchange experiment $\mathsf{KE}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n)$:

1. Two parties holding 1^n execute protocol Π. Π results in a **transcript** trans containing all the messages sent by the parties, and a **key** k that is output by each of the parties.
2. A random bit $b \leftarrow \{0,1\}$ is chosen. If $b = 0$ then choose $\hat{k} \leftarrow \{0,1\}^n$ *u.a.r*, and if $b = 1$ then set $\hat{k} := k$.
3. $\mathcal{A}$ is given trans and $\hat{k}$, and outputs a bit b'.
4. $\mathsf{KE}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n) = 1$ if $b' = b$, and 0 otherwise.

Definition 1

A key-exchange protocol Π is secure in the presence of an eavesdropper if $\forall$ PPT $\mathcal{A}$, $\exists$ negl such that

$$\Pr[\mathsf{KE}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n) = 1] < \frac{1}{2} + \mathsf{negl}(n).$$

Diffie-Hellman Key-Exchange Protocol

$(\mathbb{G}, q, g) \leftarrow \mathcal{G}$

$x \leftarrow \mathbb{Z}_q$

$h_1 := g^x \xrightarrow{\mathbb{G}, q, g, h_1}$

$y \leftarrow \mathbb{Z}_q$

$\xleftarrow{h_2} h_2 := g^y$

$k_A := h_2^x$ $\qquad$ $k_B := h_1^y$

$$k_A = k_B = k = g^{xy}.$$

$\widehat{\mathsf{KE}}^{\mathsf{eav}}_{\mathcal{A},\Pi}$ denote an experiment where if $b = 0$ the adversary is given $\hat{k} \leftarrow \mathbb{G}$.

Theorem 2

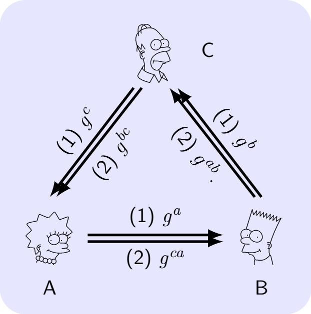
If DDH problem is hard relative to $\mathcal{G}$, then DH key-exchange protocol Π is secure in the presence of an eavesdropper (with respect to the modified experiment $\widehat{\mathsf{KE}}^{\mathsf{eav}}_{\mathcal{A},\Pi}$).

Security

Insecurity against active adversaries (Man-In-The-Middle).

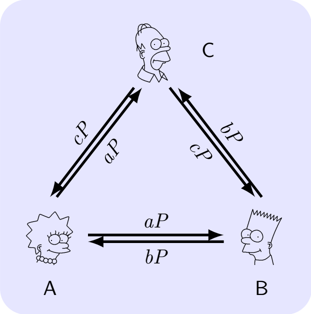
Triparties Key Exchange

DH-based KE in 2 rounds:



Key= g^{abc}.

Joux's KE in 1 round:



Key= $e(P,P)^{abc}$ in bilinear map.

Open Problem

How to exchange keys between 4 parties in one round?

Summary

- Merkle, Diffie, Hellman, Rivest, Shamir, Adleman and Rabin.
- Needham-Schroeder protocol, Diffie-Hellman key-exchange protocol.