Part II: public key crypto

Today: basic key exchange.

Recap: part I studies symmetric crypto

Alice wants to send a msg to Bob (or store file on disk)

(1) if only need data integrity: use a MAC (HMAC)

(2) if need confidentiality: use AE cipher (AES-GCM)
(nonce-based)

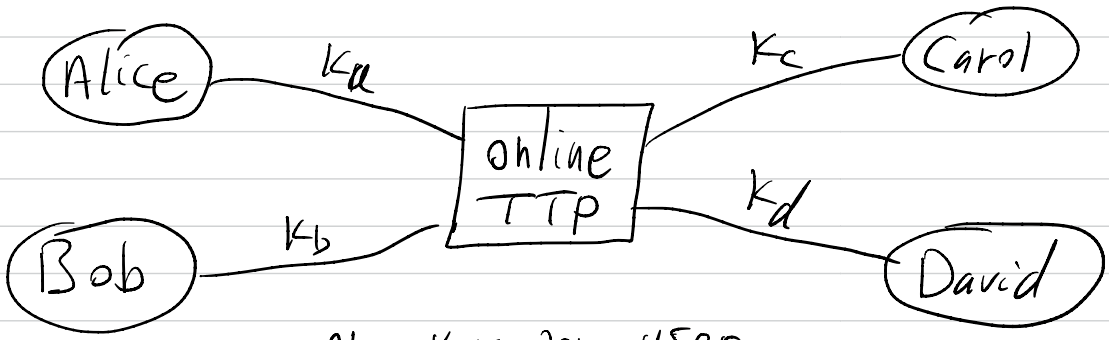
where does key k from?

Answer: key exchange protocol

Basic key exchange

method 1: online trusted 3rd party (TTP)

Setup:



one key per user.

Key exchange: a toy protocol (secure against eavesdropping)

need: CPA-secure cipher (E, D) with key space $\mathcal{K}$.

Alice wants a shared key with Bob.

Server Bob (K_b) | User Alice (K_a) | TTP (K_a, K_b)

"A wants key with B" →

$K_{ab} \xleftarrow{R} \mathcal{K}$

$c_1 := E(K_a, K_{ab})$

$c_2 := E(K_b, K_{ab})$ ← ticket

ticket ←

K_{ab} | K_{ab}

Eavesdropper sees: $E(K_a, K_{ab})$, $E(K_b, K_{ab})$

(E, D) is CPA-secure ⇒ eavesdropper learns nothing about K_{ab}.

Notes: (1) TTP is needed for every key exchange.

(2) knows all secret keys (backdoor heaven)

(3) basis of Kerberos system (windows)

Toy protocol is insecure against active attacks.

Example: replay

- attacker: record session between Alice & bank

  e.g.: A → B: pay claire $100.

- attacker replays session to bank.

  Bank thinks Alice want to pay claire again.

basic question: TTP is a problem.

can we generate a shared key w/o online TTP?

Answer: yes! starting point of pub. key crypto.

How?

- Merkle (1974): using only symmetric ciphers.

  problem: impractical! (can't be improved)

undergrad

- Need more structure: algebra
  - Diffie-Hellman (1976, stanford)
  - RSA (1977)
  - Elliptic curve crypto (1984)
  - ⋮

Project 2 looks more reasonable, maybe because your description of Project 1 is muddled terribly. Talk to me about these today.

C.S. 244
FALL 1974

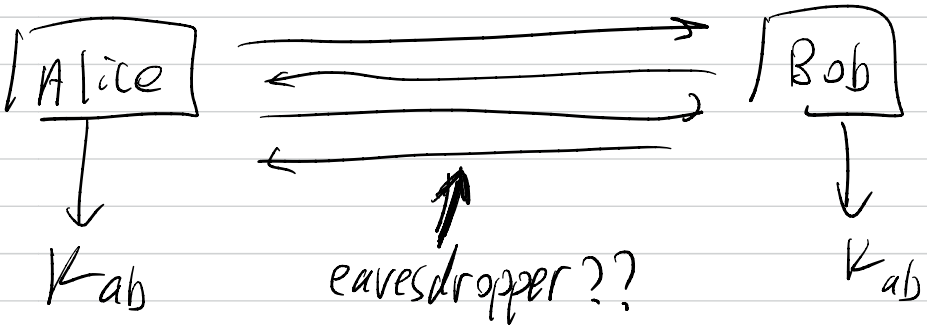
Ralph Merkle

Project Proposal

Topic: Establishing secure communications between seperate secure sites over insecure communication lines.

Assumptions: No prior arrangements have been made between the two sites, and it is assumed that any information known at either site is known to the enemy. The sites, however, are now secure, and any new information will not be divulged.

Key exchange w/o online TTP (eavesdropping security)



The basic Diffie-Hellman protocol:

Toy protocol: eavesdropping security only. (enhancements to come)

Fix a large prime p (e.g. 600 digits)

Fix an integer g s.t. $1 < g < p$.

Alice		Bob
$a \xleftarrow{R} \{1, \ldots, p-1\}$		$b \xleftarrow{R} \{1, \ldots, p-1\}$
	$A \leftarrow g^a \pmod p$ (remainder) $\longrightarrow$	
	$\longleftarrow B \leftarrow g^b \pmod p$	

$B^a = (g^b)^a \pmod p = K_{ab} = g^{ab} \pmod p = A^b = (g^a)^b \pmod p$

$\Rightarrow$ both sides obtain the same key K_{ab}

Eavesdropping security: (much more on this later)

eavesdropper sees: $p, g, g^a, g^b \pmod p$

can it compute $g^{ab} \pmod p$??

more generally: define $DH_g(g^a, g^b) = g^{ab} \pmod p$

How hard is DH_g ??

p is n-bit prime $\Rightarrow$

best known alg. (GNFS) runs in time $\tilde{O}(e^{\sqrt[3]{n}})$

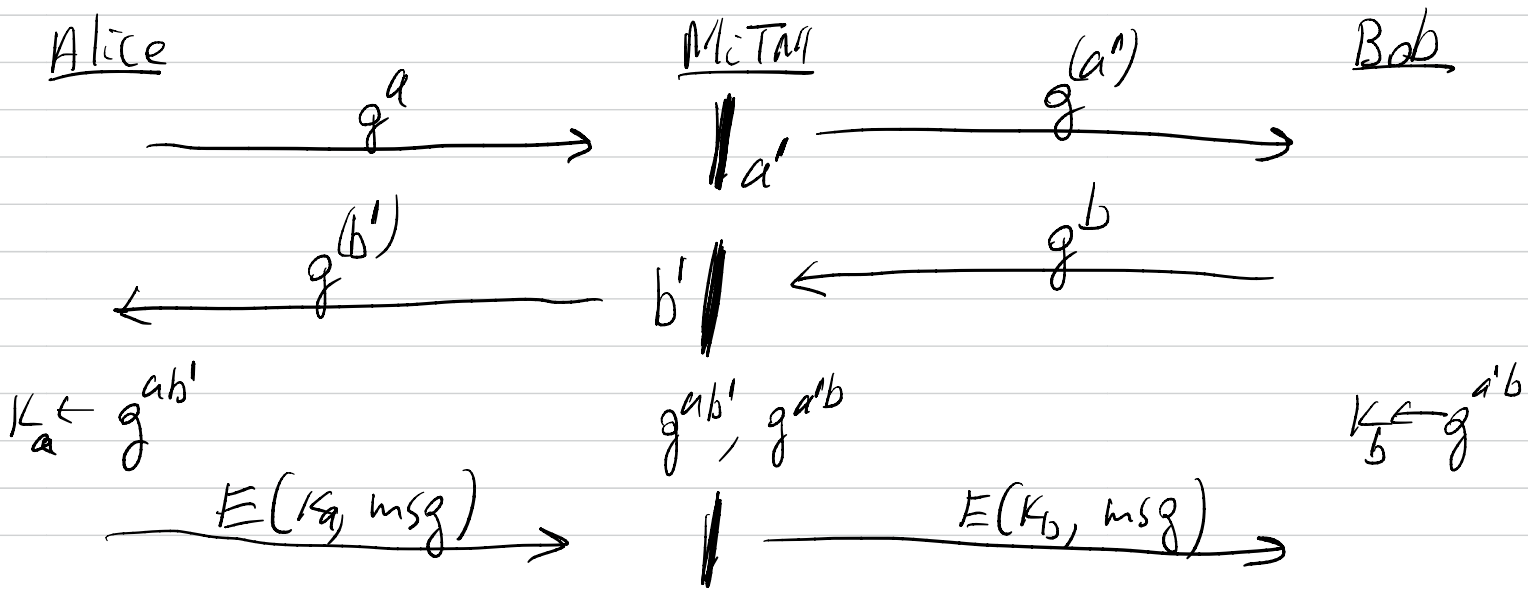
cipher key size	recommended n	ECDH n
128 bits	3072 bits	256 bits
256 bits	15360 bits	512 bits

variant of DH using n-bit prime (more on this next time)

$\Rightarrow$ transition to ECDH.

Basic DH is insecure against active attacks

Example: MiTM



on the web:

Connection - secure connection settings

The connection to this site is encrypted and authenticated using TLS 1.3, X25519, and AES_128_GCM.

ECDH

Amazon.com

Connection - secure connection settings

The connection to this site is encrypted and authenticated using TLS 1.2, ECDHE_[redacted] with X25519, and CHACHA20_POLY1305.

nytimes.com on M1

Arithmetic mod large p

h-bit integer: 

$\frac{h}{32}$ limbs

arithmetic algs: add, sub : $O(h)$

mult : $O(h^2)$

[karatsuba $O(h^{1.58})$
recent $O(h \log h)$]

Exponentiation: computing $g^x \pmod p$

repeated squaring: $g^{13} = g^{(1101)_2} = g^8 \cdot g^4 \cdot g^1 \pmod p$

Let $X = x_n x_{n-1} \cdots x_1 x_0 \in \{0,1\}^{n+1}$ be binary rep. of x.

alg.: $z \leftarrow 1$, $y \leftarrow g$

For $i = 0, 1, \ldots, n$:

if $x_i = 1$ set $z \leftarrow z \cdot y \pmod p$

$y \leftarrow y^2 \pmod p$ // $g, g^2, g^4, g^8, g^{16} \ldots$

output z

run time: $\leq (2 \cdot \log_2 x)$ multiplications.

$x \approx p \Rightarrow O(h^3)$ time