Intro to IT Security

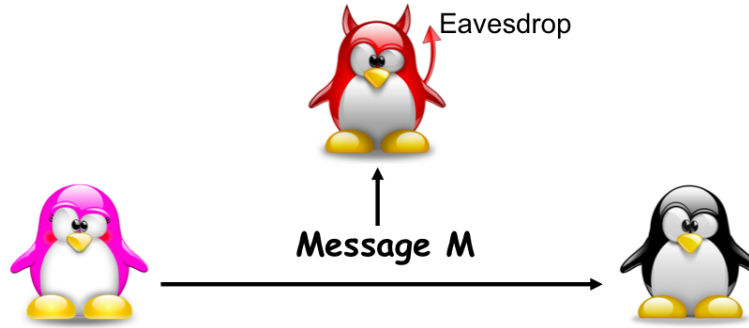
CS306C—Fall 2022

Prof. Antonio R. Nicolosi

Antonio.Nicolosi@stevens.edu

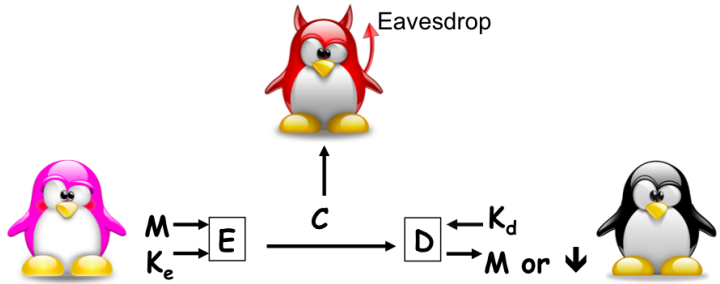
Asymmetric Cryptography

Crypto Requirements: Data Secrecy



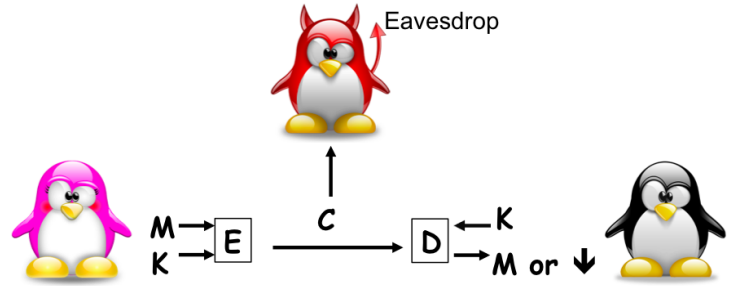
- Protect against unauthorized disclosure of the msg
  - If **A** sends a msg to **B**, no one else should understand its content

Achieving Data Secrecy: Encryption



- Notation
  - **M**: msg or plaintext
  - **C**: encrypted msg or ciphertext
  - **E**: encryption algorithm
  - **D**: decryption algorithm
  - K_e: encryption key
  - K_d: decryption key

Symmetric Encryption



- **A** and **B** share the same secret information
  - $K = K_e = K_d$: secret

Limitation of symmetric setting

- We need to agree on a secret key, before we can start communicate
- Approach 1: Key-Exchange Protocols
- Approach 2: Asymmetric Encryption

How Do Parties Share a Key?

- Use a secure physical channel
  - Meeting in person
  - Dedicated phone-line
  - USB Stick
- **Key exchange protocols**
  - parties can agree on a key over a public channel
- *Passive adversaries*
  - Eve only observes the network
  - Eve cannot change messages

Key Exchange Protocol: Merkle Puzzles

- Alice and Bob want to agree on a key
- Can only use public channels
- Eve can observe the messages that Alice sends to Bob
- Eve cannot modify the messages

Key Exchange Protocol: Merkle Puzzles

- Select n and ℓ, such that $\ell \gg \log n$
  - *E.g.*, $n = 2^{20} \approx 1M$, $\ell = 160 \Rightarrow (160 \gg 20)$
- Consider an injective hash function $H : \{0,1\}^* \rightarrow \{0,1\}^{\ell}$ (*e.g.*, SHA-1)
  - For simplicity, $H : \{0,1\}^{160} \rightarrow \{0,1\}^{160}$

Key Exchange Protocol: Merkle Puzzles

Alice:

- Chooses a subset of (say $2n$) random variables $x_1, \ldots, x_{2n} \in \{1, \ldots n^2\}$
  - $n^2 \approx 10^{12} = 1$ trillion
  - We are selecting 2 millions x_i's
  - Each x_i can be represented with 40 bits
- Chooses random prefix $p \in \{0,1\}^{120}$
  - $H_p : \{0,1\}^{40} \to \{0,1\}^{160}$
  - $x \mapsto H(p||x)$
  - H_p is 1-to-1; no collisions w.h.p
- Computes

$$\begin{aligned} a_1 &:= H_p(x_1) = H(p||x_1) \\ a_2 &:= H_p(x_2) = H(p||x_2) \\ &\vdots \\ a_{2n} &:= H_p(x_{2n}) = H(p||x_{2n}) \end{aligned}$$

- Sends $a_1, \ldots, a_{2n}, p$ to Bob

Key Exchange Protocol: Merkle Puzzles

Bob:

- Receives $a_1, \ldots, a_{2n}, p$
- Chooses $2n$ random variables $y_1, \ldots, y_{2n} \in \{1, \ldots n^2\}$
- Computes

$$
\begin{aligned}
b_1 &:= H_p(y_1) = H(p||y_1) \\
b_2 &:= H_p(y_2) = H(p||y_2) \\
&\vdots \\
b_{2n} &:= H_p(y_{2n}) = H(p||y_{2n})
\end{aligned}
$$

- Sends $b_1, \ldots, b_{2n}$ to Alice

Key Exchange Protocol: Merkle Puzzles

Alice:

- Receives $b_1, \ldots, b_{2n}$
- Finds i, j such that $a_i = b_j$
- Recovers x_i from a_i

Key Exchange Protocol: Merkle Puzzles

Bob:

- Receives $a_1, \ldots, a_{2n}$
- Finds i, j such that $a_i = b_j$
- Recovers y_j from b_j

Key Exchange Protocol: Merkle Puzzles

- W.h.p. $x_i = y_j \Rightarrow K_{AB} = x_i = y_j$
- We need to show:
  1. W.h.p. ($> 98/100$) Alice and Bob choose at least 1 common value K_{AB}
  2. Alice and Bob can find K_{AB} in **linear** time $O(n)$ (= 1 Million ops)
  3. Eve needs $O(n^2)$ (= 1 Trillion ops) time to find K_{AB}

(1) Alice and Bob have at least one k_{AB} in common

- $\Pr[x_1 = y_1] = \frac{1}{n^2}$
- $\Pr[x_1 \neq y_1] = 1 - \Pr[x_1 = y_1] = 1 - \frac{1}{n^2}$
- $\Pr[x_i \neq y_j] = 1 - \frac{1}{n^2}$

$$\Pr\left[\bigwedge_{i=1}^{2n}\bigwedge_{j=1}^{2n}(x_i \neq y_j)\right] = \text{(by independence)}$$

$$= \prod_{i=1}^{2n}\prod_{j=1}^{2n}\Pr[x_i \neq y_j] =$$

$$= \prod_{i=1}^{2n}\prod_{j=1}^{2n}\left(1 - \frac{1}{n^2}\right) =$$

$$= \left(1 - \frac{1}{n^2}\right)^{4n^2} \approx \left(\frac{1}{e}\right)^4 < 0.02$$

(1) Alice and Bob have at least one k_{AB} in common

$$\Pr[\exists\, i\,,\ \exists\, j \text{ such that } (x_i = y_j)] = \Pr\left[\bigvee_{i=1}^{2n}\bigvee_{j=1}^{2n}(x_i = y_j)\right]$$

$$= 1 - \Pr\left[\bigwedge_{i=1}^{2n}\bigwedge_{j=1}^{2n}(x_i \neq y_j)\right]$$

$$> 1 - 0.02 = 0.98 \qquad \text{(high probability!)}$$

(2) Alice and Bob can find K_{AB} in linear time in n

Assume $a_1, \ldots, a_{2n}$ and $b_1, \ldots, b_{2n}$ ordered lexicographically

Alice:

- Uses a hash table to store $a_1, \ldots, a_{2n}$

  for $i = 1$ **to** $2n$

  Insert (a_i, x_i) in the table, indexed by a_i

- Uses same hash table to look up $b_1, \ldots, b_{2n}$

  for $j = 1$ **to** $2n$

  Look-Up b_i in the table

- Uses a table to remember (a_i, x_i) pairs

(2) Alice and Bob can find K_{AB} in linear time in n

Bob:

- Uses a hash table to store $b_1, \ldots, b_{2n}$

  for $j = 1$ **to** $2n$

  Insert b_j, y_j in the table, indexed by b_j

- Uses same hash table to look up $a_1, \ldots, a_{2n}$

  for $i = 1$ **to** $2n$

  Look-Up a_i in the table

- Uses a table to remember (b_j, y_j) pairs

(3) Eve needs $O(n^2)$ time to find K_{AB}

Eve:

- Sees $a_1, \ldots, a_{2n}, b_1, \ldots, b_{2n}, p$
- Can find i, j such that $a_i = b_j$
  - $a_i = H(p||x_i)$, $b_j = H(p||y_j)$, where $x_i = y_j = K_{AB}$
- But H is one-way $\Rightarrow$ cannot invert better than brute force
  - On average, need to go through half of the possible values for $x_i \in \{1, \ldots, n^2\} \Rightarrow O(n^2)$

Definition and Notation

Let $\mathbb{G}$ be a group and let $g \in \mathbb{G}$. The set (which is in fact a subgroup) $\{0,1\}^{g^x | x \in \mathbb{Z}}$ is called *the subgroup generated by g* and is denoted with $\langle g \rangle$. The number of elements in $\langle g \rangle$ is the *order* of $\mathbb{G}$.

Definition. *A group $\mathbb{G}$ is* cyclic *if it is generated by a single element:*

$$\exists g \in \mathbb{G} \quad \text{s.t.} \quad \langle g \rangle = \mathbb{G}.$$

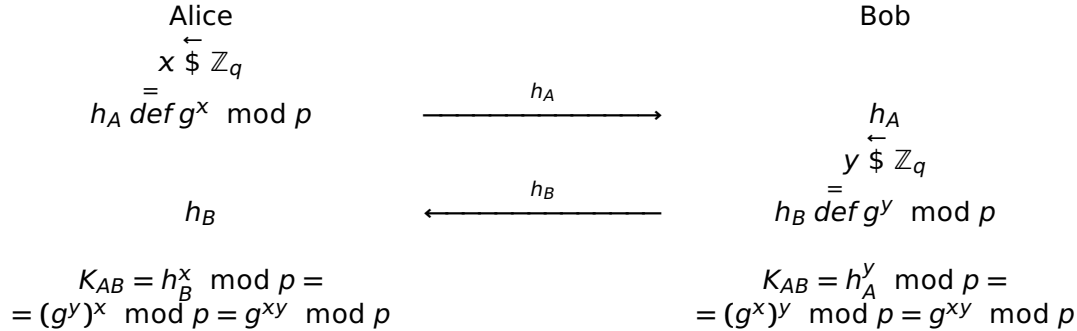
Example:

- $Z_{11} = \{0,1,2,3,4,5,6,7,8,9,10\}$
- $\mathbb{G} = QR_{11} \subset Z_{11} := \{1,3,4,5,9\}$
- $g = 3$
  - $1 \overset{\times 3}{\to} 3 \overset{\times 3}{\to} 9 \overset{\times 3}{\to} 5 \overset{\times 3}{\to} 4 \overset{\times 3}{\to} 1$ (multiplications are mod 11)

Diffie-Hellman Key Exchange

Let $\mathbb{G}$ be a cyclic group of prime order q and let $p = 2q + 1$, p also prime.

Let g be a generator of $\mathbb{G}$.



Discrete Logarithm Problem

Let $\mathbb{G}$ be a cyclic group of order q ($|q| = n$) and a let $g \in \mathbb{G}$ be a generator.

Definition. *The Discrete Logarithm (DLog) problem is hard relative to* $\mathbb{G}$ *if* $\forall$PPT$\mathcal{A}$*, there exists a negligible function* negl *such that*

$$\Pr[g^{x'} = h \mid x \xleftarrow{\$} \mathbb{Z}_q, h \stackrel{def}{=} g^x, x' = \mathcal{A}(\mathbb{G}, q, g, h)] \leq \text{negl}(n)$$

Decisional Diffie-Hellman Problem

Let $\mathbb{G}$ be a cyclic group of order q ($|q| = n$) and a let $g \in \mathbb{G}$ be a generator. Let $x, y, z \leftarrow \mathbb{Z}_q$ uniformly chosen.

Definition. *The Decisional Diffie-Hellman (DDH) problem is hard relative to* $\mathbb{G}$ *if* $\forall$PPT$\mathcal{A}$*, there exists a negligible function* negl *such that*

$$|\Pr[\mathcal{A}(\mathbb{G}, q, g, g^x, g^y, g^z) = 1] - \Pr[\mathcal{A}(\mathbb{G}, q, g, g^x, g^y, g^{xy}) = 1]| \leq \text{negl}(n)$$

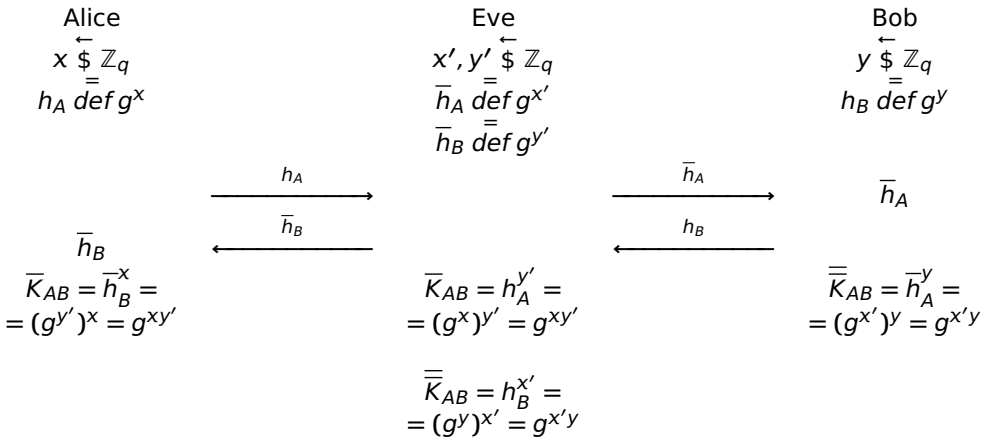
Diffie-Hellman Key Exchange

Theorem. *If the decisional Diffie-Hellman problem is hard relative to $\mathbb{G}$, the Diffie-Hellman key-exchange protocol is secure in the presence of an eavesdropper.*

Active Adversaries

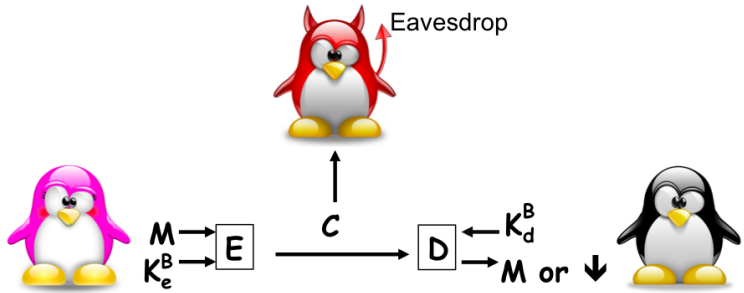
- The Diffie-Hellman key exchange protocol is insecure against main-in-the-middle attacks (active adversary)
  - The Diffie-Hellman protocol *does not provide authentication*
- In practice, use IPsec, a standardized key exchange protocol, secure against active adversaries

Man-In-The-Middle Attack*



(*) Omitting the modulo operation.

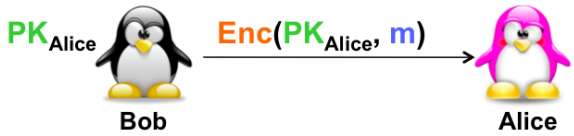
Asymmetric Setting



- **A** and **B** each have their own pair of (Public, Secret) information
  - K_e^A: public; K_d^A: secret
  - K_e^B: public; K_d^B: secret

Asymmetric Encryption

- Defined by three algorithms:
  - Gen(λ) $\rightarrow$ (SK, PK) outputs secret key SK and public key PK
  - Enc(PK, m) $\rightarrow$ c encrypt m using public key PK
  - Dec(SK, c) $\rightarrow$ m or $\perp$ decrypt c using SK



Asymmetric Encryption Scheme: Correctness

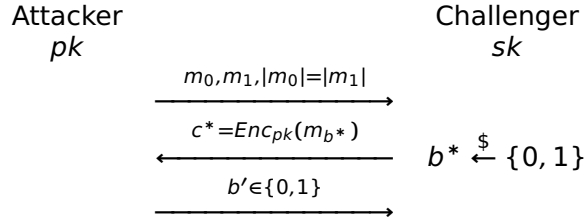
$$\Pr[Dec_{sk}(Enc_{pk}(m)) = m] = 1$$

where the probability is over $(sk, pk) \leftarrow KG(1^n)$, and the randomness used in the encryption algorithm Enc

Security Against Eavesdropping Attacks

Given an asymmetric encryption scheme $\Pi = (KG, Enc, Dec)$, and an adversary $\mathcal{A}$, consider the following game.

Let $(pk, sk) = KG(1^n)$:

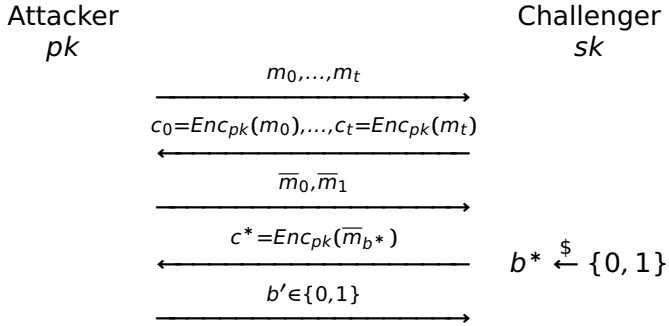


The output of the experiment is 1 if $b' = b^*$, and 0 otherwise.

Security Against Chosen-Plaintext Attacks (CPA)

Given an asymmetric encryption scheme $\Pi = (KG, Enc, Dec)$, and an adversary $\mathcal{A}$, consider the following experiment.

Let $(pk, sk) = KG(1^n)$:



The output of the experiment is 1 if $b' = b^*$, and 0 otherwise.

CPA ⇒ Indistinguishable encryption

Any scheme that has indistinguishable encryptions under chosen-plaintex attack, also has indistinguishable encryption in the presence of an eavesdropper.

Indistinguishable encryption ⇒ CPA

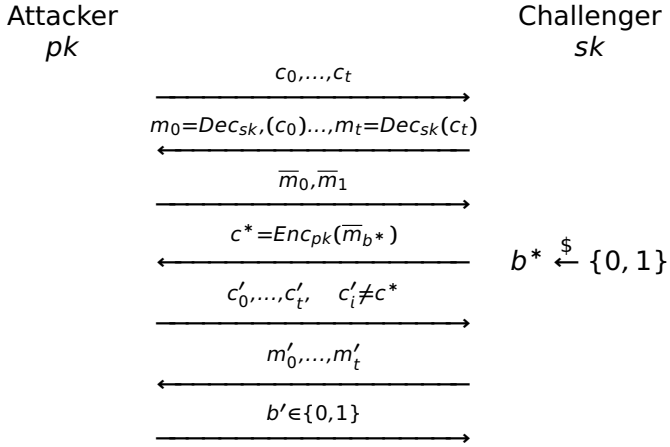
Any scheme that has indistinguishable encryptions in the presence of an eavesdropper, also has indistinguishable encryption under chosen-plaintex attack.

Note that in the asymmetric setting, the adversary has access to the public key, and thus can create any ciphertext of her choice without the need of an encryption oracle.

Security Against Chosen-Ciphertext Attacks (CCA)

Given an asymmetric encryption scheme $\Pi = (KG, Enc, Dec)$, and an adversary $\mathcal{A}$, consider the following experiment.

Let $(pk, sk) = KG(1^n)$:



The output of the experiment is 1 if $b' = b^*$, and 0 otherwise.

Hybrid Encryption

Let $\Pi = (KG, Enc, Dec)$ be an asymmetric encryption scheme and let $\Pi' = (KG', Enc', Dec')$ be a secret-key encryption scheme. To encrypt a message m

- The receiver creates its own (pk, sk) pair and publish pk
- The sender chooses a random secret key k, and encrypts k using Enc and the public key pk of the receiver
- The sender then encrypts m using Enc' and the secret key k

Hybrid Encryption Security

Theorem. *If* Π *is a CPA-secure asymmetric encryption scheme and* Π' *is a private key encryption scheme that has indistinguishable encryption in the presence of an eavesdropper, then* Π^{hy} *is a CPA-secure asymmetric encryption scheme.*