EECS 575: Advanced Cryptography
Fall 2022
Lecture 2

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Modelling secure communication
- Information-theoretic security

Agenda for this lecture

- Announcements
- Modelling secure communication
- Information-theoretic security

Announcements

- Homework/exam schedule is (tentatively) done:
  - HW1: put online 9/5, due 9/16
    HW2: put online 9/16, due 9/30
    Take-home exam #1: put online 10/3, due 10/10
    HW3: put online 10/7, due 10/21
    HW4: put online 10/21, due 11/4
    HW5: put online 11/4, due 11/18
    HW6: put online 11/16, due 11/28*****
    Take-home exam #2: put online 11/28, due 12/5

Agenda for this lecture

- Announcements
- Modelling secure communication
- Information-theoretic security

Modelling Secure Communication

Eve

algorithm $E : \boldsymbol{C} \rightarrow \boldsymbol{*}$

Alice $\longrightarrow$ Bob

algorithm $A : \boldsymbol{M} \rightarrow \boldsymbol{C}$

algorithm $B : \boldsymbol{C} \rightarrow \boldsymbol{M}$

Desired functionality: for any m in $\boldsymbol{M}$, $B(A(\mathrm{m})) = \mathrm{m}$

Desired security?

Can just set $E = B$ and learn any message. Hmm…

Fixing the Model

Eve

algorithm E : $\boldsymbol{C} \rightarrow \boldsymbol{*}$

Alice $\longrightarrow$ Bob

algorithm A : $\boldsymbol{M} \rightarrow \boldsymbol{C}$

algorithm B : $\boldsymbol{C} \rightarrow \boldsymbol{M}$

<u>Kerchoff's Law</u>:
A cryptographic algorithm should be secure even if its description is public.

What if the algorithm B was secret?

Security through obscurity

Symmetric-Key Encryption

Eve

algorithm $E : \boldsymbol{C} \to *$

Alice $\longrightarrow$ Bob

Enc : $\boldsymbol{K} \times \boldsymbol{M} \to \boldsymbol{C}$

Dec : $\boldsymbol{K} \times \boldsymbol{C} \to \boldsymbol{M}$

Instead, allow both Enc and Dec to take a ***key*** k.
K is generated by a randomized algorithm Gen

Desired functionality: for any m in $\boldsymbol{M}$ and k in $\boldsymbol{K}$, Dec(k, Enc(k, m)) = m

Questions:

- In this model, how must $|\boldsymbol{M}|$ and $|\boldsymbol{C}|$ be related?
- Can we infer anything about $|\boldsymbol{K}|$ in relation to $|\boldsymbol{M}|$ or $|\boldsymbol{C}|$?

Security of Symmetric-Key Encryption

What security properties might we want here?

Eve

algorithm $E : \boldsymbol{C} \rightarrow *$

Alice $\longrightarrow$ Bob

Enc : $\boldsymbol{K} \times \boldsymbol{M} \rightarrow \boldsymbol{C}$

Dec : $\boldsymbol{K} \times \boldsymbol{C} \rightarrow \boldsymbol{M}$

Seeing the ciphertext should be no better than seeing *nothing at all*

Agenda for this lecture

- Announcements
- Modelling secure communication
- Information-theoretic security

Shannon Secrecy

Definition 2.1 (Shannon secrecy)**.** A symmetric-key encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ with message space $\mathcal{M}$ and ciphertext space $\mathcal{C}$ is *Shannon secret with respect to a probability distribution D over $\mathcal{M}$* if for all $\bar{m} \in \mathcal{M}$ and all $\bar{c} \in \mathcal{C}$,

$$\Pr_{m \leftarrow D,\ k \leftarrow \mathsf{Gen}}[m = \bar{m} \mid \mathsf{Enc}_k(m) = \bar{c}] = \Pr_{m \leftarrow D}[m = \bar{m}].$$

The scheme is *Shannon secret* if it is Shannon secret with respect to every distribution D over $\mathcal{M}$.

Rewriting Shannon Secrecy

Definition 2.1 (Shannon secrecy)**.** A symmetric-key encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ with message space $\mathcal{M}$ and ciphertext space $\mathcal{C}$ is *Shannon secret with respect to a probability distribution* D over $\mathcal{M}$ if for all $\bar{m} \in \mathcal{M}$ and all $\bar{c} \in \mathcal{C}$,

$$\Pr_{m \leftarrow D,\ k \leftarrow \mathsf{Gen}}[m = \bar{m} \mid \mathsf{Enc}_k(m) = \bar{c}] = \Pr_{m \leftarrow D}[m = \bar{m}].$$

The scheme is *Shannon secret* if it is Shannon secret with respect to every distribution D over $\mathcal{M}$.

Perfect Secrecy

Definition 2.2 (Perfect secrecy). A symmetric-key encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ with message space $\mathcal{M}$ and ciphertext space $\mathcal{C}$ is *perfectly secret* if for all $m_0, m_1 \in \mathcal{M}$ and all $\bar{c} \in \mathcal{C}$,

$$\Pr_{k \leftarrow \mathsf{Gen}}[\mathsf{Enc}_k(m_0) = \bar{c}] = \Pr_{k \leftarrow \mathsf{Gen}}[\mathsf{Enc}_k(m_1) = \bar{c}].$$

The One-Time Pad

Perfect Secrecy of the One-Time Pad

Theorem 2.4. *The one-time pad is a perfectly secret symmetric-key encryption scheme.*

Proof:

Questions to think about

If we replaced XOR with AND in the one-time pad, would it still be a valid encryption scheme? Would it be perfectly secret?