CS306: Introduction to IT Security

Fall 2020

Lecture 3: Perfect Secrecy

Instructor: **Nikos Triandopoulos**

September 15, 2020

STEVENS
INSTITUTE of TECHNOLOGY
THE INNOVATION UNIVERSITY®

Assignment Project Exam Help

https://powcoder.com

3.0 Announcements

Add WeChat powcoder

CS306: Lab sections schedule

- labs
  - CS306-Lx Thursdays **ZOOM ID: LAB SPECIFIC!**

x	B	C	D	E	F
time	9:30 - 10:20	11:00 - 11:50	12:30 - 13:20	14:00 - 14:50	15:30 - 16:20
Zoom ID	91573945614	93061161569	94976630644	92834271191	94520991826
TAs	Dean, Joseph, Joshua, Uday	Dean, Devharsh, Joseph, Joshua	Dean/Devharsh, Joshua, Mohammad, Uday	Devharsh, Joseph, Mohammad, Uday	Dean, Joseph, Mohammad, Uday

CS306: Other announcements

- Lab #2 this Thursday
- Homework #1 this Friday

CS306: Tentative Syllabus

Week	Date	Topics	Reading	Assignment
1	**Sep 1**	**Introduction**	**Lecture 1**	**-**
2	**Sep 8**	**Symmetric-key encryption**	**Lecture 2**	**Lab 1**
3	Sep 15	Symmetric-key crypto II		
4	Sep 22	Public-key crypto I		
5	Sep 29	Public-key crypto II		
6	Oct 6	Access control & authentication		
-	Oct 13	**No class (Monday schedule)**		
7	Oct 20	**Midterm**	All materials covered	

CS306: Tentative Syllabus (continued)

Week	Date	Topics	Reading	Assignment
8	Oct 27	Software & Web security		
9	Nov 3	Network security		
10	Nov 10	Database security		
11	Nov 17	Cloud security		
12	Nov 24	Privacy		
13	Dec 1	Economics		
14	Dec 8	Legal & ethical issues		
15	Dec 10 (or later)	**Final** (closed "books")	All materials covered*	

* w/ focus on what covered after midterm

Last week

- Introduction to the field of IT security
  - Basic concepts and terms
  - Symmetric encryption

Today

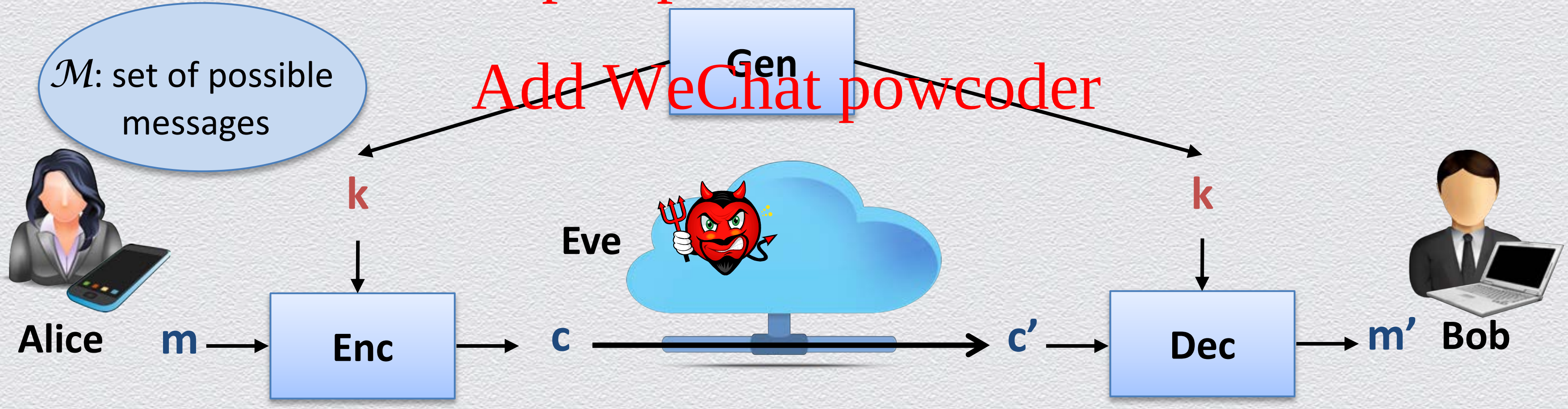
- Symmetric-key Cryptography
  - Perfect secrecy
  - The One-Time Pad cipher
- Demo
  - Why encryption matters?
  - Using the Wireshark packet analyzer

3.1 Perfect secrecy

Security tool: Symmetric-key encryption scheme

Abstract cryptographic primitive, **a.k.a. cipher**, defined by

- a **message space** $\mathcal{M}$; and
- a triplet of algorithms **(Gen, Enc, Dec)**
  - Gen, Enc are probabilistic algorithms, whereas Dec is deterministic
  - Gen outputs a uniformly random key k (from some key space $\mathcal{K}$)



Perfect correctness

For any $k \in \mathcal{K}$, $m \in \mathcal{M}$ and any ciphertext c output of $\mathrm{Enc}_k(m)$,

it holds that

$$\Pr[\,\mathrm{Dec}_k(c) = m\,] = 1$$

Towards defining perfect security

- defining security for an encryption scheme is not trivial
  - e.g., what we mean by << Eve "cannot learn" m (from c) >> ?
- our setting so far is a random experiment
  - a message m is chosen according to $\mathcal{D}_{\mathcal{M}}$
  - a key k is chosen according to $\mathcal{D}_{\mathcal{K}}$
  - $\mathrm{Enc}_k(m) \rightarrow c$ is given to the adversary

how to define security?

Attempt 1: Protect the key k!

- Security means that

  the adversary should **not** be able to **compute the key k**

- Intuition
  - it'd better be the case that the key is protected!...

necessary condition

- Problem
  - this definition fails to exclude clearly insecure schemes
  - e.g., the key is never used, such as when $\mathrm{Enc}_k(m) := m$

but not sufficient condition!

Attempt 2: Don't learn m!

- Security means that

  the adversary should **not** be able to **compute the message m**

- Intuition
  - it'd better be the case that the message m is not learned...

- Problem
  - this definition fails to exclude clearly undesirable schemes
  - e.g., those that protect m partially, i.e., they reveal the least significant bit of m

Attempt 3: Learn nothing!

- Security means that

  the adversary should **not** be able to **learn any information about m**

- Intuition
  - it seems close to what we should aim for perfect secrecy…
- Problem
  - this definition ignores the adversary's prior knowledge on $\mathcal{M}$
  - e.g., distribution $\mathcal{D}_{\mathcal{M}}$ may be known or estimated
    - m is a valid text message, or one of "`attack`", "`no attack`" is to be sent

Attempt 4: Learn nothing more!

- Security means that

  the adversary should **not** be able to **learn any <u>additional</u> information on m**

- How can we formalize this?

Alice **m**

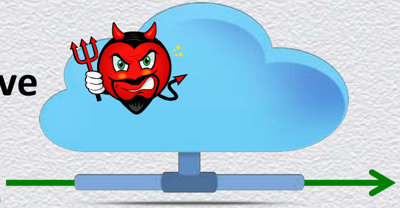
Enc$_k$(m) → c

Eve

$$\mathbf{m} = \begin{cases} \texttt{attack} & \text{w/ prob. } 0.8 \\ \texttt{no attack} & \text{w/ prob. } 0.2 \end{cases}$$

Eve's view remains the same!

Eve



c

$$\mathbf{m} = \begin{cases} \texttt{attack} & \text{w/ prob. } 0.8 \\ \texttt{no attack} & \text{w/ prob. } 0.2 \end{cases}$$

Two equivalent views of perfect secrecy

a posteriori = a priori $\sim$ **C is independent of M**

For every $\mathcal{D}_\mathcal{M}$, m $\in \mathcal{M}$ and c $\in \mathcal{C}$, for which Pr [C = c] > 0, it holds that

$$\Pr[\ M = m \mid C = c\ ] = \Pr[\ M = m\ ]$$

For every m, m' $\in \mathcal{M}$ and c $\in \mathcal{C}$, it holds that

$$\Pr[\ \mathrm{Enc}_K(m) = c\ ] = \Pr[\ \mathrm{Enc}_K(m') = c\ ]$$

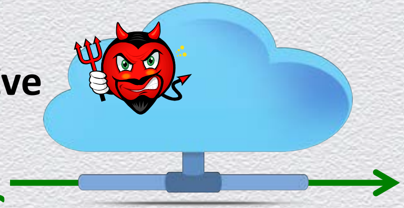
random experiment
$\mathcal{D}_\mathcal{M} \rightarrow$ m = M
$\mathcal{D}_\mathcal{K} \rightarrow$ k = K
$\mathrm{Enc}_k(m) \rightarrow$ c = C

Eve

m = { `attack` w/ prob. 0.8; `no attack` w/ prob. 0.2

Eve's view remains the same!

Eve



c

m = { `attack` w/ prob. 0.8; `no attack` w/ prob. 0.2

Perfect secrecy (or information-theoretic security)

Definition 1

A symmetric-key encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$, is **perfectly secret** if for every $\mathcal{D}_{\mathcal{M}}$, every message m ∈ $\mathcal{M}$ and every ciphertext c ∈ C for which Pr [C = c] > 0, it holds that

$$\mathbf{Pr[\ M = m\ |\ C = c\ ] = Pr\ [\ M = m\ ]}$$

- intuitively
  - the *a posteriori* probability that any given message m was actually sent is the **same** as the *a priori* probability that m would have been sent
  - observing the ciphertext reveals **nothing (new)** about the underlying plaintext

Alternative view of perfect secrecy

Definition 2

A symmetric-key encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$, is **perfectly secret** if for every messages m, m' $\in \mathcal{M}$ and every c $\in$ C, it holds that

$$\Pr[\, \mathrm{Enc}_K(m) = c \,] = \Pr[\, \mathrm{Enc}_K(m') = c \,]$$

- intuitively
  - the probability distribution $\mathcal{D}_C$ **does not depend** on the plaintext
  - i.e., M and C are **independent** random variables
  - the ciphertext contains "**no information**" about the plaintext
  - "**impossible to distinguish**" an encryption of **m** from an encryption of **m'**

3.2 The one-time pad

The one-time pad: A perfect cipher

A type of "substitution" cipher that is "absolutely unbreakable"

- invented in 1917 Gilbert Vernam and Joseph Mauborgne
- "substitution" cipher
  - **individually** replace plaintext characters with **shifted** ciphertext characters
  - **independently** shift each message character in a **random** manner
    - to encrypt a plaintext of length n, use n uniformly random keys $k_1, \ldots, k_n$
- "absolutely unbreakable"
  - **perfectly secure** (when used correctly)
  - based on message-symbol specific **independently random** shifts

The one-time pad (OTP) cipher

Fix n to be any positive integer; set $\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0,1\}^n$

- **Gen**: choose n bits uniformly at random (each bit independently w/ prob. .5)
  - Gen $\rightarrow \{0,1\}^n$
- **Enc**: given a key and a message of equal lengths, compute the bit-wise XOR
  - $\mathrm{Enc}(k, m) = \mathrm{Enc}_k(m) \rightarrow k \oplus m$ (i.e., mask the message with the key)
- **Dec**: compute the bit-wise XOR of the key and the ciphertext
  - $\mathrm{Dec}(k, c) = \mathrm{Dec}_k(c) := k \oplus c$
- Correctness
  - trivially, $k \oplus c = k \oplus k \oplus m = 0 \oplus m = m$

OTP is perfectly secure (using Definition 2)

For all n-bit long messages m_1 and m_2 and ciphertexts c, it holds that

$$\Pr[\, E_K(m_1) = c \,] \quad = \quad \Pr[\, E_K(m_2) = c \,],$$

where probabilities are measured over the possible keys chosen by Gen.

Proof

- events "$Enc_K(m_1) = c$", "$m_1 \oplus K = c$" and "$K = m_1 \oplus c$" are equal-probable
- K is chosen at random, irrespectively of m_1 and m_2, with probability 2^{-n}
- thus, the ciphertext does not reveal anything about the plaintext

OTP characteristics

A "substitution" cipher

- encrypt an n-symbol m using n uniformly random "shift keys" $k_1, k_2, \ldots, k_n$

2 equivalent views

- $\mathcal{K} = \mathcal{M} = \mathcal{C}$
- "shift" method

	view 1		**view 2**
$\mathcal{K} = \mathcal{M} = \mathcal{C}$	$\{0,1\}^n$	or	G, (G,+) is a group
"shift" method	bit-wise XOR ($m \oplus k$)		addition/subtraction (m +/- k)

Perfect secrecy

- since each shift is random, every ciphertext is equally likely for any plaintext

Limitations (on efficiency)

- "shift keys" (1) are **as long as messages** & (2) **can be used only once**

Perfect, but impractical

In spite of its perfect security, OTP has two notable weaknesses

- the key has to be **as long as** the plaintext
  - limited applicability
  - key-management problem
- the key **cannot be reused** (thus, the "one-time" pad)
  - if reused, perfect security is not satisfied
    - e.g., reusing a key once, leaks the XOR of two plaintext messages
    - this type of leakage can be devastating against secrecy

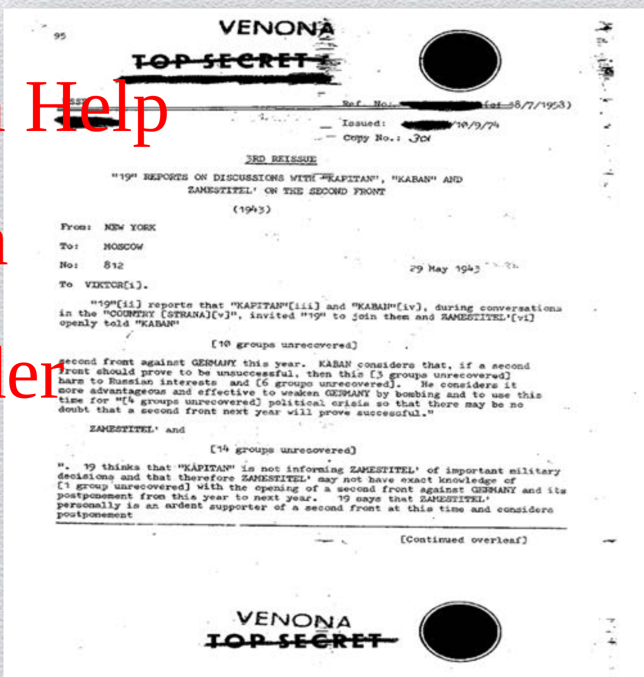
These weakness are detrimental to secure communication

- securely distributing fresh long keys is as hard as securely exchanging messages…

Importance of OTP weaknesses

Inherent trade-off between efficiency / practicality Vs. perfect secrecy

- historically, OTP has been used efficiently & insecurely
  - repeated use of one-time pads compromised communications during the cold war
    - NSA decrypted Soviet messages that were transmitted in the 1940s
    - that was possible because the Soviets reused the keys in the one-time pad scheme
- modern approaches resemble OTP encryption
  - efficiency via use of pseudorandom OTP keys
  - “almost perfect” secrecy



95

VENONA

TOP SECRET

[redacted]

Ref. No.: [redacted] (of 18/7/1953)

Issued: [redacted]/10/9/74

Copy No.: 301

3RD REISSUE

"19" REPORTS ON DISCUSSIONS WITH "KAPITAN", "KABAN" AND ZAMESTITEL' ON THE SECOND FRONT

(1943)

From: NEW YORK

To: MOSCOW

No: 812

29 May 1943

To VIKTOR[i].

"19"[ii] reports that "KAPITAN"[iii] and "KABAN"[iv], during conversations in the "COUNTRY [STRANA][v]", invited "19" to join them and ZAMESTITEL'[vi] openly told "KABAN"

[10 groups unrecovered]

second front against GERMANY this year. KABAN considers that, if a second front should prove to be unsuccessful, then this [3 groups unrecovered] harm to Russian interests and [6 groups unrecovered]. He considers it more advantageous and effective to weaken GERMANY by bombing and to use this time for "[4 groups unrecovered] political crisis so that there may be no doubt that a second front next year will prove successful."

ZAMESTITEL' and

[14 groups unrecovered]

". 19 thinks that "KAPITAN" is not informing ZAMESTITEL' of important military decisions and that therefore ZAMESTITEL' may not have exact knowledge of [1 group unrecovered] with the opening of a second front against GERMANY and its postponement from this year to next year. 19 says that ZAMESTITEL' personally is an ardent supporter of a second front at this time and considers postponement

[Continued overleaf]

VENONA

TOP SECRET