CS306: Introduction to IT Security

Fall 2020

Le crecy

Instructor: **Nikos**

September 15, 2020

1870

STEVENS
INSTITUTE *of* TECHNOLOGY
THE INNOVATION UNIVERSITY®

ounce

CS306: Lab sections schedule

- labs
  - CS306-Lx Thursdays

ZOOM ID: LAB SPECIFIC!

x	B			E	F
time	9:30 - 10:20			:00 - 14:50	15:30 - 16:20
Zoom ID	91573945614	93061161569	9497	271191	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			
4	Sep 22			
5	Sep 29	Public-key cr		
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			
11	Nov 17			
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

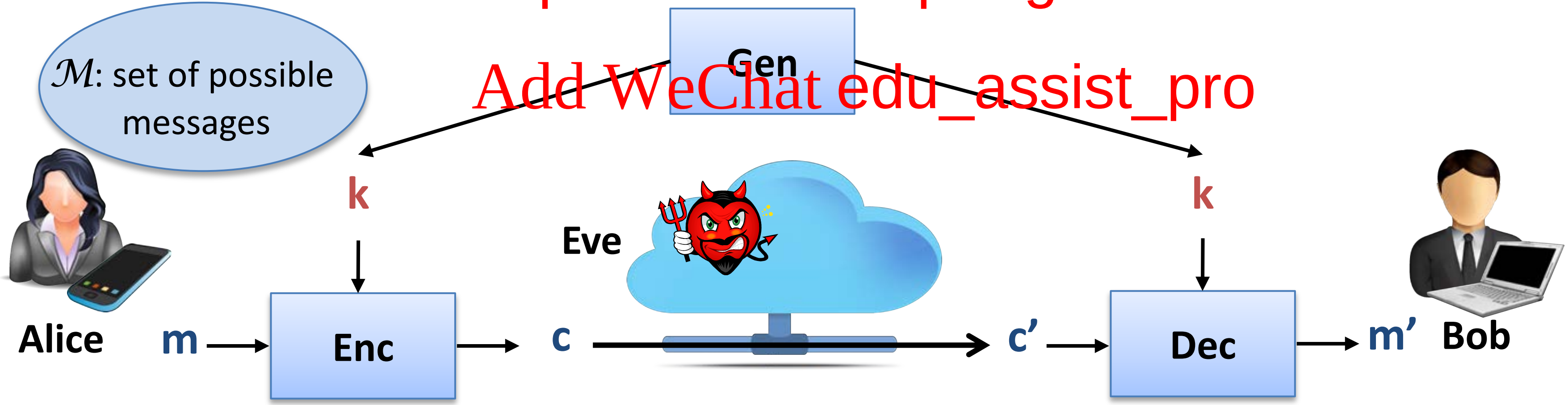
- Symmetric-key Cryptography
  - Perfect secrecy
  - The One-Time Pad cipher
- Demo
  - Why encryption ma
  - Using the Wireshark packet analyzer

ect se

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 unif ey space $\mathcal{K}$)



Perfect correctness

For any k ∈ $\mathcal{K}$, m ∈ $\mathcal{M}$ and any ciphertext c output of Enc_k(m),

it holds that

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 chose
  - a key k is chosen according to $\mathcal{D}_{\mathcal{K}}$
  - $\mathrm{Enc}_k(m) \to c$ 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 c

necessary condition

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

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 c ned…

- 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**

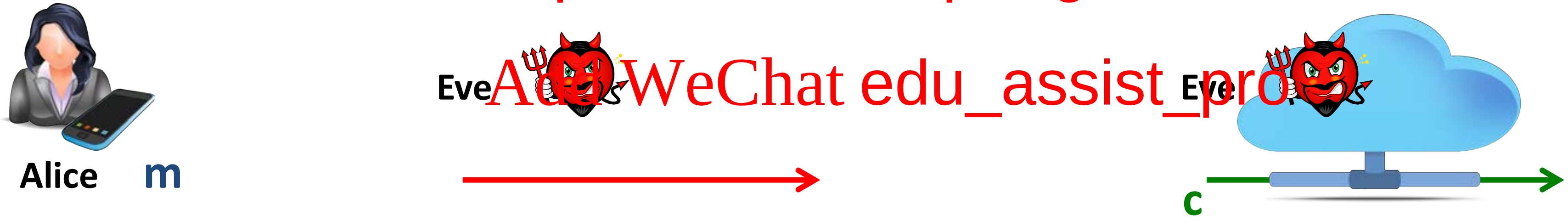
- Intuition
  - it seems close to w ecy…
- Problem
  - this definition ignores the adversary's prior knowledge on $\mathcal{M}$
  - e.g., distribution $\mathcal{D}_{\mathcal{M}}$ may be known or estimated
    - m is a valid text message, or one of "`attack`", "`no attack`" is to be sent

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 formali



$\mathrm{Enc}_k(m) \longrightarrow c$

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

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

Two equivalent views of perfect secrecy

a posteriori = a priori ~ **C is independent of M**

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

Pr[M = m | C = c] =

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

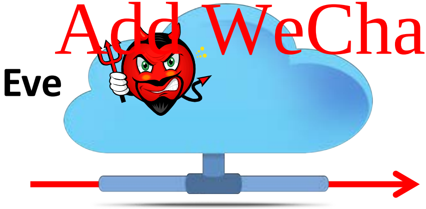
= c] = Pr[Enc$_K$(m′) = c]

random experiment

$\mathcal{D}_{\mathcal{M}} \rightarrow$ **m = M**

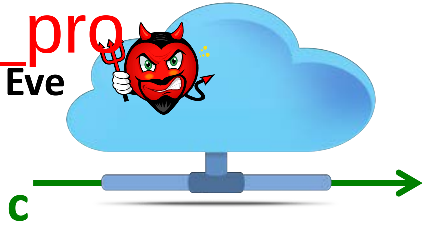
$\mathcal{D}_{\mathcal{K}} \rightarrow$ k = K

Enc$_k$(m) → c = C



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

the same!



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

Pr[m]

- intuitively

  - the *a posteriori* probability that any give s 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’ ∈ $\mathcal{M}$ and every c ∈ C, it holds that

Pr[E ’) = c]

- intuitively
  - the probability distribution $\mathcal{D}_C$ **does not** 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’**

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 ciphertext characters
  - **independently** shif **om** manner
    - to encrypt a plaintext of length n, use dom keys $k_1, . . . , k_n$
- “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 → $\{0,1\}^n$
- **Enc**: given a key and mpute the bit-wise XOR
  - $\mathrm{Enc}(k, m) = \mathrm{Enc}_k($ essage with the key)
- **Dec**: compute the bit-wise XOR of the k hertext
  - $\mathrm{Dec}(k, c) = \mathrm{Dec}_k(c) := k \oplus c$
- 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 “$\mathrm{Enc}_K(m_1) = c$”, “$m_1 \oplus K = c$” c” are equal-probable
- K is chosen at random, irrespectively , 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

vie

bit

2 G, (G,+) is a group

raction (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 p
- the key **cannot be reu**

  - if reused, perfect security is not satisfie

    - e.g., reusing a key once, leaks the XO xt 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 du
    - NSA decrypted S 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