CS 255: Course Intro

Intro. to Cryptography

Web page: cs255.stanford.edu

Textbook + MOOC available online

Assignments: 4 HWs, 2 programming projects

Late days: 3 free late days

TA email: cs255ta@stanford.edu

Sections: Friday, recommended

Other security courses:

- CS 155 → CS 356
- CS 255 → CS 355
- CS 251 (Fall)

Goals: how crypto works and how to use it correctly

Cryptography is everywhere!

→ This Zoom room: TLS encryption

Crypto in use

- TLS, SSH
  1. session setup — pub-key (ElGamal, RSA) / certificates
     secret key initialization btwn server, browser
  2. use shared key to encrypt traffic
     symmetric cipher
     For privacy, data integrity
- Secure chat: Signal, iMessage
- at-rest (filesystem) encryption: dmcrypt, FileVault, Bitlocker
- Wireless: 802.11 (WEP, WEP2, WEP3), 4G, 5G, Bluetooth
- User auth: password management, 2-factor auth (WebAuthn)
- Payments: credit card → Apple Pay, Blockchain
- other applications: elections, auctions

Things to remember

→ In cryptography, no security through obscurity

Goal: cryptosystem should be secure even if source code is open

only secret: short key (128 bits, 16 bytes)

Course organization

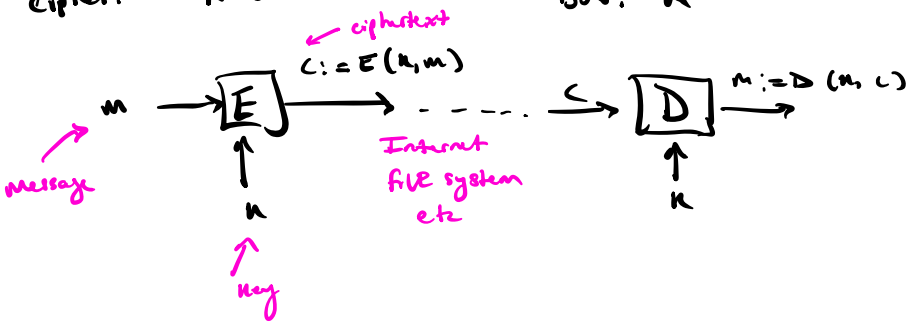
① using a shared key for confidentiality + data integrity

② session setup using public key encryption, digital signatures

③ Protocol: session setup, zero knowledge proofs, etc

Symmetric Encryption

cipher: Alice: K Bob: K



Def: A cipher def. over (K, M, C) is a pair of "efficient" algorithms (E, D)

$E: K \times M \to C$ $\quad D: K \times C \to M$

s.t. $\forall m \in M, \forall k \in K: \; D(k, E(k, m)) = m$

"efficient": polynomial time in message length, or runs in 1ms

note: enc. alg. E can be randomized ← run same alg twice, may get diff outputs on same inputs

dec. alg. D is always deterministic

⟹ No security requirements! (yet)

Oldest cipher: substitution

key: $K = \begin{bmatrix} a \to m \\ b \to g \\ c \to w \\ \vdots \\ z \to a \end{bmatrix}$ $\quad |K| = 26! \approx 2^{88}$

enc. of plaintext m = "bcza" is $C = E(K, m) =$ "gwom"

Caesar cipher (w/ key): shifts by 3

$\begin{bmatrix} a \to d \\ b \to e \\ c \to f \\ \vdots \\ z \to c \end{bmatrix}$

To break: ① Freq. of English letters

"e" : 12.7% of the time

"t" : 9.1%

"a" : 8.1%

⋮

"q"

"x"

② Freq of pairs of letters (digrams)

"th", "he", "in", "an" ...

③ Trigrams

"the" ...

⇒ Obtain entire key

⇒ ciphertext only attack!

A "secure" cipher: one-time pad (OTP)

Vernam, 1917

$M = C = \{0,1\}^n$ (all n-bit strings)

$K = \{0,1\}^n$

secret key = random bit string as long as the messages

$C := E(K, m) = K \oplus m$

$D(K, C) = K \oplus C$

$\Rightarrow D(K, E(K, m)) = K \oplus (K \oplus m)$

$= (K \oplus K) \oplus m = 0 \oplus m = m$

ex. msg: 0100110

key: 1101100

CT: 1001010

Very fast enc./dec. !!!

Problem: very long keys!

(hard to use - key sharing method can be used to share message)

Goal: keys are 128 or 256 bits

Is OTP a "secure" cipher?

What is a "secure" cipher?

Shannon 1949

Goal: a cipher is secure if ciphertext reveals no "info" about plaintext

Def: a cipher (E, D) over K, M, C has perfect secrecy if

$\forall m_0, m_1 \in M \quad (len(m_0) = len(m_1)), \quad \forall c \in C$

$$Pr[E(k, m_0) = c] = Pr[E(k, m_1) = c]$$

where k is uniform in K $(k \xleftarrow{R} K)$

Given intercepted ciphertext c, attacker can't tell if msg is m_0 or m_1

($\forall m_0, m_1 \Rightarrow$ attacker learns "nothing" about message)

$\Rightarrow$ if $len(m_0) \neq len(m_1)$, no guarantee

$\Rightarrow$ a cipher with perfect secrecy need not hide the message length

↑ problems

Theorem: OTP has perfect secrecy

Proof: $\forall m \in M, \quad c \in C$

$$Pr[E(k, m) = c] = \frac{|\{k \in K \text{ where } E(k, m) = c\}|}{|K|} = \frac{|\{k \in K \text{ where } k \oplus m = c\}|}{2^n} = \frac{1}{2^n}$$

if $k \oplus m = c$ then $k = m \oplus c$ $\Rightarrow$ one key where $k \oplus m = c$

So $\forall m \in M, c \in C$: $Pr[E(k, m) = c] = \frac{1}{2^n}$

So thm holds.

$\Rightarrow$ No CT only attacks on OTP!

Bad news thm:

Every cipher (E, D) over (K, M, C) w/ perfect secrecy must also satisfy $|K| \geq |M|$

$\Rightarrow$ $\text{len}(k) \geq \text{len}(m)$