WELCOME!

Introduction

Cryptography is Magic

History of Cryptography

Math fundamentals

Course Objectives

- Learn how cryptographic primitives work
- Use them correctly, and reason about security

Administrative Details

- Course website: https://courses.grainger.illinois.edu/cs498ac3/fa2020/

- Has syllabus, instructor and TA info, office hours

- IMPORTANT: **Join Piazza!** piazza.com/illinois/fall2020/ececs498ac/home

I strongly encourage class participation.
If you don't understand something in class, please interrupt me and ask questions.
Please make abundant use of office hours.

SSL/TLS

SSL/TLS

Two parts.

- **Handshake protocol**: Use *public key encryption* to establish shared secret key

- **Record layer:** Transmit data using shared secret key
  secret-key encryption

SSL/TLS

Two parts.

- **Handshake protocol**: Use *public key encryption* to establish shared secret key

- **Record layer:** Transmit data using shared secret key
  secret-key encryption

We will: -- see how these encryption schemes work.
-- understand why we think these are unbreakable.

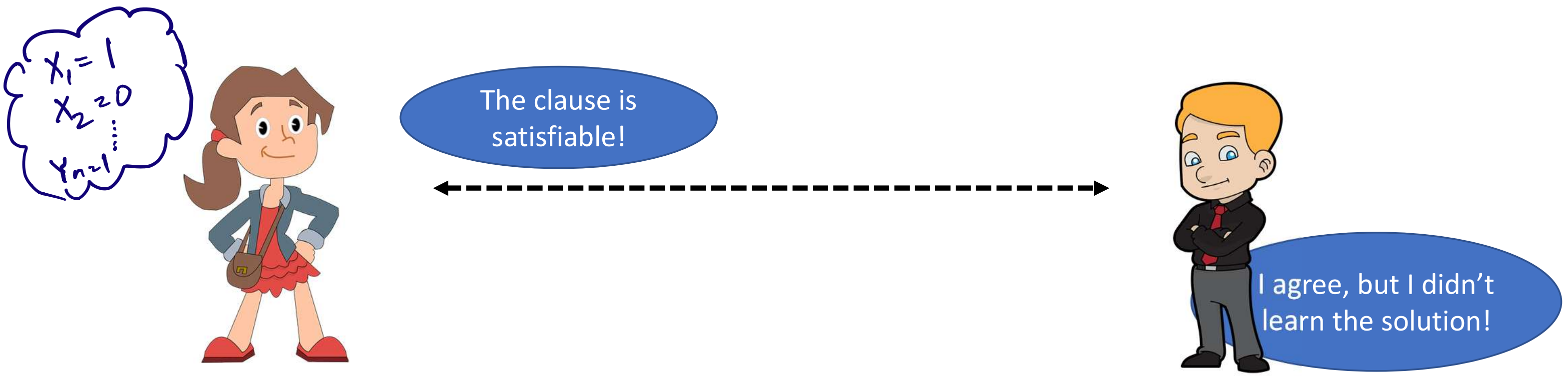
The Magic of Cryptography

Key Exchange

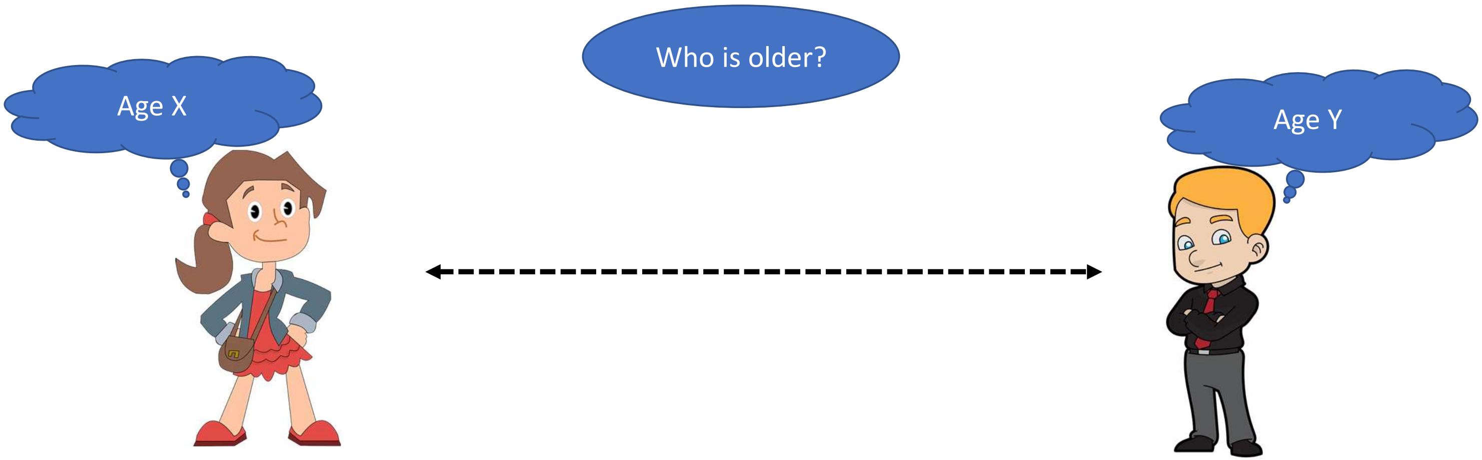
Zero-Knowledge Proofs

Given a SAT formula:

$$(X_1 \vee X_2 \vee \cdots \vee X_n) \wedge (Y_1 \vee X_2 \vee \cdots \vee X_n) \wedge (X_1 \vee Y_2 \vee \cdots \vee X_n) \wedge (Y_1 \vee Y_2 \vee \cdots \vee X_n) \wedge \cdots \wedge (Y_1 \vee Y_2 \vee \cdots \vee Y_n).$$



Secure Computation



x_2 x_3

x_1 f . . . . x_n

History

Symmetric Ciphers

Substitution Ciphers

Key

a → g

b → z

c → o

d → r

e → b

.....

z → f

a bad cab → g zgr ogz

$$K: \left| \begin{array}{l} A \to ?\ \overset{g}{\underline{26}} \\ B \to \end{array} \right|$$

$$\left| \begin{array}{l} A \to ?\ 26 \\ \quad\quad\quad \times \\ B \to ?\ 25 \\ \quad\quad\quad \times \\ C \to ?\ 24 \\ \quad \vdots \end{array} \right|$$

Poll

- What is the size of key space in the substitution cipher assuming 26 letters?

1. 26^2
2. $26!$
3. 2^{26}
4. 26

Substitution Ciphers are Easy to Break!

UKBYBIPOUZBCUFEEBORUKBYBHOBBRFESPVKBWFOFERVNBCVBZPRUBOFERVNBCVBPCYYFVUFO
FEIKNWFRFIKJNUPWRFIPOUNVNIPUBRNCUKBEFWWFDNCHXCYBOHOPYXPUBNCUBOYNRVNIWN
CPOJIOFHOPZRVFZIXUBORJRUBZRBCHNCBBONCHRJZSFWNVRJRUBZRPCYZPUKBZPUNVPWPCYVF
ZIXUPUNFCPWRVNBCVBRPYYNUNFCPWWJUKBYBIPOUZBCUIPOUNVNIPUBRNCHOPYXPUBNCUB
OYNRVNIWNCPOJIOFHOPZRNCRVNBCUNENVVFZIXUNCHPCYVFZIXUPUNFCPWZPUKBZPUNVR

B	36	→ E
N	34	
U	33	→ T
P	32	→ A
C	26	

NC	11	→ IN
PU	10	→ AT
UB	10	
UN	9	

digrams

UKB	6	→ THE
RVN	6	
FZI	4	

trigrams

Substitution Ciphers are Easy to Break!

UKBYBIPOUZBCUFEEBORUKBYBHOBBRFESPVKBWFOFERVNBCVBZPRUBOFERVNBCVBPCYYFVUFO
FEIKNWFRFIKJNUPWRFIPOUNVNIPUBRNCUKBEFWWFDNCHXCYBOHOPYXPUBNCUBOYNRVNIWN
CPOJIOFHOPZRVFZIXUBORJRUBZRBCHNCBBONCHRJZSFWNVRJRUBZRPCYZPUKBZPUNVPWPCYVF
ZIXUPUNFCPWRVNBCVBRPYYNUNFCPWWJUKBYBIPOUZBCUIPOUNVNIPUBRNCHOPYXPUBNCUB
OYNRVNIWNCPOJIOFHOPZRNCRVNBCUNENVVFZIXUNCHPCYVFZIXUPUNFCPWZPUKBZPUNVR

B	**36**	➔ E
N	**34**	
U	**33**	➔ T
P	**32**	➔ A
C	**26**	

NC	**11**	➔ IN
PU	**10**	➔ AT
UB	**10**	
UN	**9**	

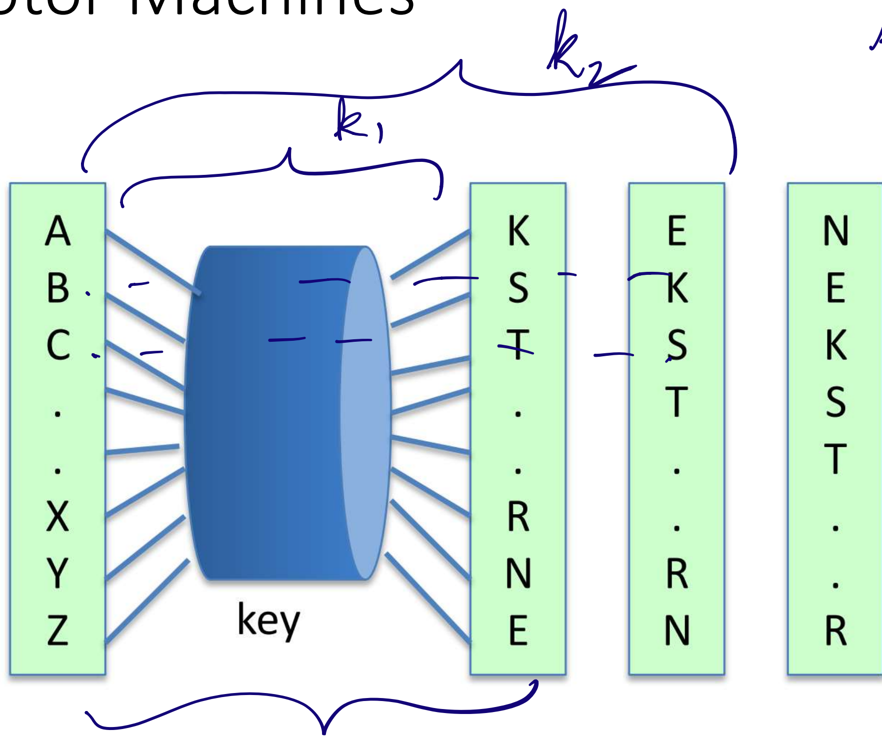
digrams

UKB	**6**	➔ THE
RVN	**6**	
FZI	**4**	

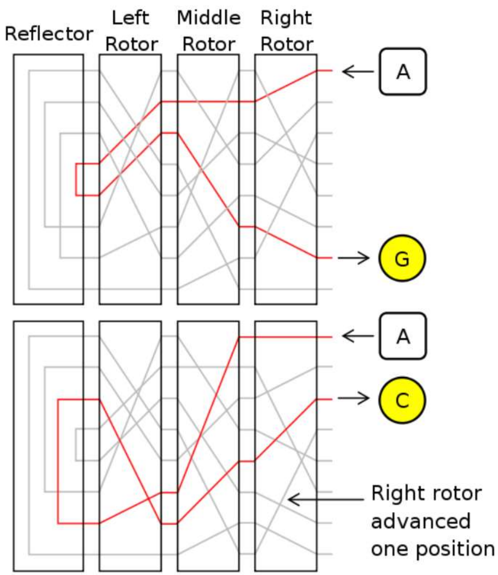
trigrams

Rotor Machines

k_2 : k_1, shifted



Rotor Machines: Advanced (The Enigma)



Encryption Standards

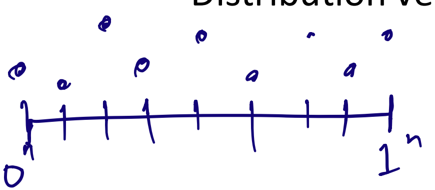
- Data Encryption Standard (DES): 2^{56} keys
- Advanced Encryption Standard (AES): used today
- And many others…

Mathematical Background

Discrete Probability

- S : finite set (e.g., $S = \{0,1\}^n$)
- A probability distribution Pr over S is a function Pr: S → [0,1] such that $\Sigma_{x \in S} \Pr(x) = 1$

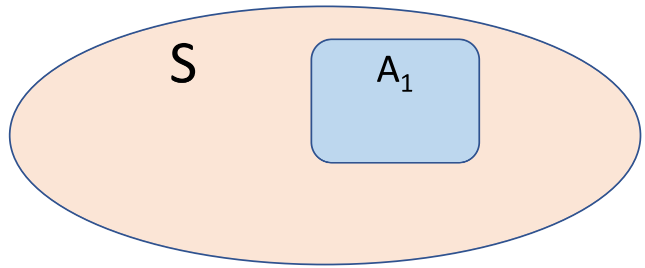
- Examples
  - Uniform distribution → $S = \{0,1\}$ $\Pr[0] = \Pr[1] = \frac{1}{2}$
    → $S = \{0,1\}^n$
    $\{000\ldots0, 00\ldots1, \ldots\ldots 11111\}$
    $\forall x \in S \; \Pr[x] = \frac{1}{2^n}$
  - Point distribution
  - Distribution vector



$S = \{0,1\}^n$
$\Pr[x] = 1$ for $x = 1010\ldots1$, $\Pr[x] = 0$ for all other $x \in S$.

Events

- For a set $A \subseteq S$, $\Pr[A] = \Sigma_{x \in A} \Pr(x)$
- The set A is called an event



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

$A = 0^{n/2} \ldots\ldots \quad \underbrace{00\ldots0}_{n/2}$

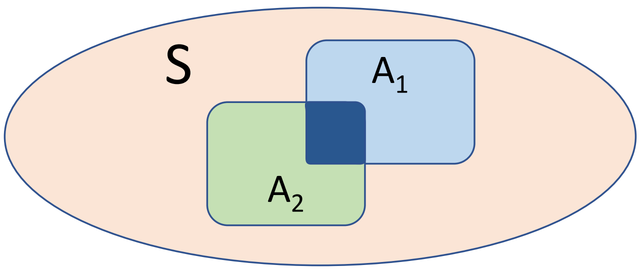
$\{0^{n/2}0\ldots0,\ 0^{n/2}0\ldots1 \ldots\ldots 0^{n/2}1^{n/2}\} \subset S$

$\Pr_{x \leftarrow S}[x \in A] = \frac{1}{2^{n/2}}$ (uniform distribution over S)

Events

- For a set $A \subseteq S$, $\Pr[A] = \Sigma_{x \in A} \Pr(x)$
- The set A is called an event

- For events A_1 and A_2, $\Pr[A_1 \cup A_2] \leq \Pr[A_1] + \Pr[A_2]$



Random Variables

- A random variable X is a function $X : \cancel{U}\ S \longrightarrow V$

- Let $\cancel{U}$ S be some set, e.g. $\cancel{U}\ S = \{0,1\}^n$

- We write $r \longleftarrow \cancel{U}\ S$ to denote a uniform random variable over $\cancel{U}$ S

  for all $a \in \cancel{U}\ S$: $\Pr[\, r = a \,] = 1/|\cancel{U}\ S| = \dfrac{1}{2^n}$

Randomized Algorithms

- We will make extensive use of randomized algorithms
- Deterministic algorithm: y ⟵ A(m)
- Randomized algorithm: y ⟵ A(m; r)
- Eg, to encrypt message m, we will sample r ⟵ ~~U~~ and output Enc(m;r)

S

$\{0,1\}^n$

Independent Events

- Events A and B are independent if Pr[A and B] = Pr[A] · Pr[B]

- Random variables X,Y taking values in $\overset{\mathcal{S}}{\cancel{V}}$ are independent if

  $\forall$(a, b) $\in$ $\underset{\mathcal{S}}{\cancel{V}}$: Pr [X=a and Y=b] = Pr [X=a] · Pr [Y=b]

Independent Events

$0 \oplus 0 = 0$

$0 \oplus 1 = 1$

$1 \oplus 0 = 1$

$1 \oplus 1 = 0$

- XOR: bitwise addition mod 2. Example –
- If Y some ~~random~~ arbitrary (not necessarily uniform) variable over $\{0,1\}^n$,

  and X an *independent* uniform variable on $\{0,1\}^n$

  Then $Z := Y \oplus X$ is a uniform variable on $\{0,1\}^n$

message $Y = 1\,1\,1 \ldots\ldots 1$ ← arbitrary

$\oplus$ random $X = \overset{b_1}{0}\,\overset{b_2}{1}\,1 \ldots\ldots 0$ ← uniform

random $Z = 1\,0\,0 \ldots\ldots 1$ ← uniform

The One-Time Pad

Symmetric Ciphers

Symmetric Ciphers : One Time Pad

- A cipher defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$

  is a pair of efficient algorithms **(E, D)** where

  E: $\mathcal{K} \times \mathcal{M} \rightarrow \mathcal{C}$

  D: $\mathcal{K} \times \mathcal{C} \rightarrow \mathcal{M}$

  such that for all $m \in \mathcal{M}$, $k \in \mathcal{K}$, $\underline{\mathbf{D}(k, \overline{\mathbf{E}(k, m)}) = m}$

  (Correctness)

  $E(k, m) \longrightarrow c$

  then $D(k, c) \longrightarrow m$

The One-Time Pad

- Provably Secure Cipher

  $\mathcal{K} = \{0,1\}^n$, $\mathcal{M} = \{0,1\}^n$, $\mathcal{C} = \{0,1\}^n$

- Key is sampled uniformly from the set $\mathcal{K} = \{0,1\}^n$

  i.e. the key is a random bit string as long as the message

- E (k, m) = $\underbrace{k}_{=X} \oplus \underbrace{m}_{=Y}$
- D (k, c) = $k \oplus c$
- Check correctness

We want:

$$D(k, \underbrace{E(k, m)}_{c = (k \oplus m)}) = m$$

$$k \oplus c = k \oplus k \oplus m = m$$

The One-Time Pad

- Example

$m = 10101011101$

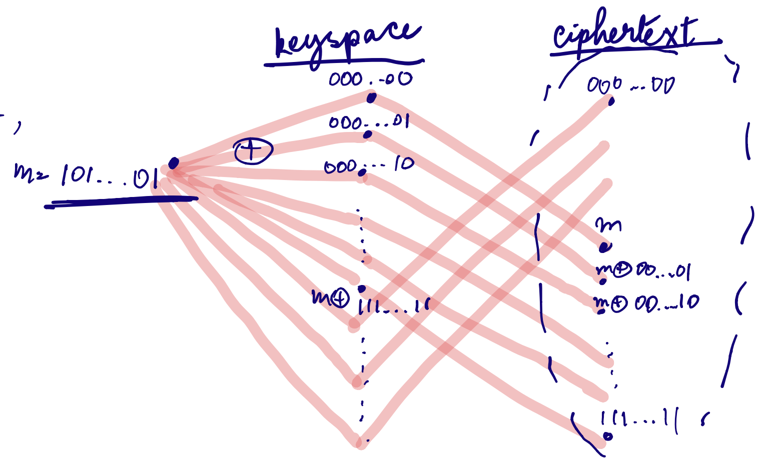
random

$\oplus$ $\xrightarrow{\text{random}}$ $k = 1010111010$

random

- Check correctness

- What about security? Intuitively,



The One-Time Pad

- Let's define security for a symmetric cipher. (perfect secrecy)

<u>Defn 1:</u> $\forall\ m_0, m_1 \in \mathcal{M}$ (of equal size, i.e. $|m_0| = |m_1|$) and $\forall c \in C$

$$\Pr_{k \leftarrow K}[\,E(k,m_0) = c\,] \quad = \quad \Pr_{k \leftarrow K}[\,E(k,m_1) = c\,]$$

An attacker, given c, cannot guess m.

$c_1 = k_1 \oplus m$

$c_2 = k_2 \oplus c_1 = (k_2 \oplus k_1) \oplus m$

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

$C = \{0,1\}^n$.

The One-Time Pad

- Theorem: The one-time pad satisfies <u>Defn 1</u> (perfect secrecy).

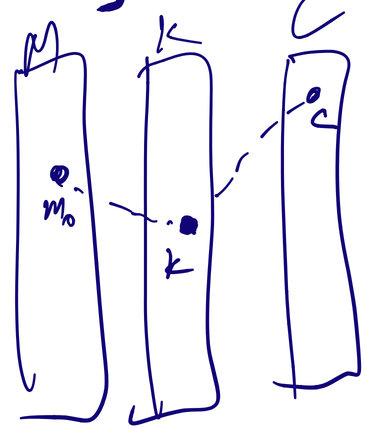
$\forall m_0, m_1, \forall c$

$$\Pr_{k \leftarrow K}[E(k, m_0) = c] = \Pr_{k \leftarrow K}[E(k, m_1) = c]$$

Fix arbitrary m_0 & arbitrary c.

$$\Pr_{k \leftarrow K}[E(k, m_0) = c] = \frac{1}{2^n}$$

Similarly, $\Pr_{k \leftarrow K}[E(k, m_1) = c] = \frac{1}{2^n}$



$c = m_0 \oplus k$

$k = m_0 \oplus c$

The One-Time Pad: Disadvantage

- Observe: $|\mathcal{K}| = |\mathcal{M}|$

- That means to send a long file, you need to share a long key.
  - And for every file, you need a new key. Why?

- Can you have $|\mathcal{K}| < |\mathcal{M}|$?

$\nexists$ any encryption scheme where $|K|<|M|$.

- Shannon: No ☹. For perfect secrecy, you need $|\mathcal{K}| >= |\mathcal{M}|$. Why?

Prove: if $|K|<|M|$, then $\exists\, m_0, m_1 \in M$, $\exists\, c \in C$

s.t. $\Pr_{k \leftarrow K}[E(k, m_0) = c] \neq \Pr_{k \leftarrow K}[E(k, m_1) = c]$

Conclusion

computational

- Looking ahead: *perfect* secrecy unnecessary, can relax it.

computationally bounded

- Assume *hard problems* that cannot be solved by adversaries (i.e. we will assume P! = NP, and in fact something stronger).

- Under these assumptions, we will achieve *provable* security.

- *Conditional* secrecy:
  hardness of problem ------ => secrecy of the scheme.