

# Introduction to Encryption

Ruta Jawale

July 1, 2019

# Announcements

## Announcements

Introduction

Objectives

Symmetric Key  
Encryption

Ciphertext IND

IND-KPA

IND-CPA

IND-CCA1

IND-CCA2

Achieve IND-CPA

One Time Pad

AES Block Cipher

Summary

- Homework 1 due in a week (7/8)
- Project 1 due in about a week (7/11)
- Midterm 1 in two weeks (7/15)
  - Attend lecture and discussion sections to learn material to appear on Midterm 1

# Premise: Alice wants to ask Bob on a date...



...but doesn't want anyone else to know or mess up her plans!

Let's help her setup a secure method of communication.

Announcements

Introduction

Objectives

Symmetric Key  
Encryption

Ciphertext IND

IND-KPA

IND-CPA

IND-CCA1

IND-CCA2

Achieve IND-CPA

One Time Pad

AES Block Cipher

Summary

# Alice's security specifications

Announcements

Introduction

Objectives

Symmetric Key  
Encryption

Ciphertext IND

IND-KPA

IND-CPA

IND-CCA1

IND-CCA2

Achieve IND-CPA

One Time Pad

AES Block Cipher

Summary

We want CIA. (*No, not the Central Intelligence Agency.*)

- Confidentiality

- only Alice and Bob should know the message

- Integrity

- Alice's message was not modified or tampered with

- Authentication

- Bob should be able to verify Alice sent the message

# Meet Alice's adversaries

Eve the Eavesdropper



Likes: Reading messages  
Dislikes: Confidentiality

Mallory the Manipulator



Likes: Altering messages  
Dislikes: Integrity/Authenticity

For now, we'll focus on giving Eve a hard time.

Announcements

Introduction

Objectives

Symmetric Key  
Encryption

Ciphertext IND

IND-KPA

IND-CPA

IND-CCA1

IND-CCA2

Achieve IND-CPA

One Time Pad

AES Block Cipher

Summary

# Achieve confidentiality to upset Eve

Announcements

Introduction

Objectives

Symmetric Key  
Encryption

Ciphertext IND

IND-KPA

IND-CPA

IND-CCA1

IND-CCA2

Achieve IND-CPA

One Time Pad

AES Block Cipher

Summary

Eve dislikes confidential secrets. How can we ensure that Eve can't read Alice's correspondence? (*Rhetorical question*)



Let's encrypt Alice's message!





# Types of encryption

Encryption key



Decryption key



- Symmetric key encryption  = 
  - same private key for encryption and decryption
- Asymmetric key encryption   $\neq$  
  - separate public encryption key and private decryption key

Both types of encryption achieve confidentiality, necessary to annoy Eve. For now, we'll focus on symmetric encryption.

# Learning objectives

Announcements

Introduction

Objectives

Symmetric Key  
Encryption

Ciphertext IND

IND-KPA

IND-CPA

IND-CCA1

IND-CCA2

Achieve IND-CPA

One Time Pad

AES Block Cipher

Summary

- Learn how to make formal security arguments
  - Specifically prove or disprove that a scheme is IND-KPA or IND-CPA secure
- Build intuition from formal security proofs
  - For example, understand what it means to be IND-CPA secure



# Symmetric key encryption (*think of API or “blueprint”*)

Announcements

Introduction

Objectives

Symmetric Key  
Encryption

Ciphertext IND

IND-KPA

IND-CPA

IND-CCA1

IND-CCA2

Achieve IND-CPA

One Time Pad

AES Block Cipher

Summary



Icon Credit: Nikita Golubev

**Gen**( $1^n$ )  $\rightarrow k$ :  $\underbrace{\quad}_{n \text{ times}}$

Input:  $1^n = \underbrace{1 \dots 1}_{n \text{ times}}$ , allows its runtime to depend on length of the key

$|k| = n$

Output: secret key  $k$

**Enc**( $k, m$ )  $\rightarrow c$ :

Input: secret key  $k$ , message or plaintext  $m$

Output: ciphertext  $c$

**Dec**( $k, c$ )  $\rightarrow m$ :

Input: secret key  $k$ , ciphertext  $c$

Output: message  $m$

# Symmetric key encryption



How do we know that our encryption works?

$$\forall m, k \quad \mathbf{Dec}(k, \mathbf{Enc}(k, m)) = m$$

We call this the correctness property!

Is the correctness property enough for encryption to be confidential? No, we need a security guarantee.

Announcements

Introduction

Objectives

Symmetric Key  
Encryption

Ciphertext IND

IND-KPA

IND-CPA

IND-CCA1

IND-CCA2

Achieve IND-CPA

One Time Pad

AES Block Cipher

Summary

# How do establish security? Games!

We phrase security of encryption schemes as a game between a challenger and an adversary. If no adversary can win the game with probability greater than random chance, then we consider the scheme secure.

Challenger

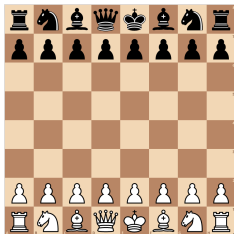


Photo Credit: lichess

Adversary



Announcements

Introduction

Objectives

Symmetric Key  
Encryption

Ciphertext IND

IND-KPA

IND-CPA

IND-CCA1

IND-CCA2

Achieve IND-CPA

One Time Pad

AES Block Cipher

Summary

# Ciphertext Indistinguishability as Games

Announcements

Introduction

Objectives

Symmetric Key  
Encryption

Ciphertext IND

IND-KPA

IND-CPA

IND-CCA1

IND-CCA2

Achieve IND-CPA

One Time Pad

AES Block Cipher

Summary

- Indistinguishability under Known Plaintext Attack (IND-KPA)
- Indistinguishability under Chosen Plaintext Attack (IND-CPA)
- Indistinguishability under (Non-Adaptive) Chosen Ciphertext Attack (IND-CCA1)
- Indistinguishability under (Adaptive) Chosen Ciphertext Attack (IND-CCA2)

# IND-KPA Secure

Announcements

Introduction

Objectives

Symmetric Key  
Encryption

Ciphertext IND

IND-KPA

IND-CPA

IND-CCA1

IND-CCA2

Achieve IND-CPA

One Time Pad

AES Block Cipher

Summary



Challenger  $\mathcal{C}$



Adversary  $\mathcal{A}$

*Phases*

*setup*

$k \leftarrow \mathbf{Gen}(1^n)$

*challenge cipher*

$b \xleftarrow{\$} \{0, 1\}$

$c^* \leftarrow \mathbf{Enc}(k, m_b^*)$

*send bit*

*determine win*

If  $b = b'$ ,  $\mathcal{A}$  wins.

$m_0^*, m_1^*$

←

$c^*$

→

$b'$

←

# IND-KPA Secure

Announcements

Introduction

Objectives

Symmetric Key

Encryption

Ciphertext IND

IND-KPA

IND-CPA

IND-CCA1

IND-CCA2

Achieve IND-CPA

One Time Pad

AES Block Cipher

Summary



Challenger  $\mathcal{C}$   
 $k \leftarrow \mathbf{Gen}(1^n)$



Adversary  $\mathcal{A}$

*Phases*  
*setup*

*challenge cipher*

$b \xleftarrow{\$} \{0, 1\}$

$c^* \leftarrow \mathbf{Enc}(k, m_b^*)$

*send bit*

*determine win*

If  $b = b'$ ,  $\mathcal{A}$  wins.

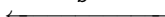
$m_0^*, m_1^*$



$c^*$



$b'$



$\forall$  adversaries  $\mathcal{A}$ ,  $\Pr[\mathcal{A} \text{ wins game}] \leq \frac{1}{2} + \text{negligible}$

Why  $\frac{1}{2}$ ? Some adversary  $\mathcal{A}$  could guess bit  $b$ . They have probability  $\frac{1}{2}$  to succeed. We don't consider this an "attack" on our encryption scheme.

# IND-KPA Secure

Announcements

Introduction

Objectives

Symmetric Key

Encryption

Ciphertext IND

IND-KPA

IND-CPA

IND-CCA1

IND-CCA2

Achieve IND-CPA

One Time Pad

AES Block Cipher

Summary



Challenger  $\mathcal{C}$   
 $k \leftarrow \mathbf{Gen}(1^n)$



Adversary  $\mathcal{A}$

*Phases*  
*setup*

*challenge cipher*

$b \xleftarrow{\$} \{0, 1\}$

$c^* \leftarrow \mathbf{Enc}(k, m_b^*)$

*send bit*

*determine win*

If  $b = b'$ ,  $\mathcal{A}$  wins.

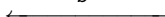
$m_0^*, m_1^*$



$c^*$



$b'$



$\forall$  adversaries  $\mathcal{A}$ ,  $\Pr[\mathcal{A} \text{ wins game}] \leq \frac{1}{2} + \text{negligible}$

What could *negligible* be? Say some adversary  $\mathcal{A}$  decides to brute force the key  $k$ . The attacker has probability  $\frac{1}{2^n}$  to succeed. That's a negligible amount.

# IND-CPA secure



*Phases*

Challenger  $\mathcal{C}$

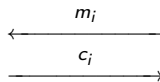
Adversary  $\mathcal{A}$

*setup*

$k \leftarrow \text{Gen}(1^n)$

*encrypt plaintext*

$c_i \leftarrow \text{Enc}(k, m_i)$

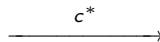
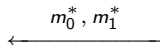


for  $i \in \text{poly}(n)$

*challenge cipher*

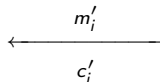
$b \xleftarrow{\$} \{0, 1\}$

$c^* \leftarrow \text{Enc}(k, m_b^*)$



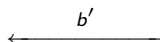
*encrypt plaintext*

$c_i \leftarrow \text{Enc}(k, m'_i)$



for  $i \in \text{poly}(n)$

*send bit*



*determine win*

If  $b = b'$ ,  $\mathcal{A}$  wins.

Announcements

Introduction

Objectives

Symmetric Key  
Encryption

Ciphertext IND

IND-KPA

**IND-CPA**

IND-CCA1

IND-CCA2

Achieve IND-CPA

One Time Pad

AES Block Cipher

Summary



# IND-CPA secure

Announcements

Introduction

Objectives

Symmetric Key

Encryption

Ciphertext IND

IND-KPA

**IND-CPA**

IND-CCA1

IND-CCA2

Achieve IND-CPA

One Time Pad

AES Block Cipher

Summary

*Phases*

*setup*

*encrypt plaintext*

*challenge cipher*

*encrypt plaintext*

*send bit*

*determine win*



Challenger  $\mathcal{C}$   
 $k \leftarrow \text{Gen}(1^n)$

$c_i \leftarrow \text{Enc}(k, m_i)$

$b \xleftarrow{\$} \{0, 1\}$

$c^* \leftarrow \text{Enc}(k, m_b^*)$

$c_i \leftarrow \text{Enc}(k, m'_i)$

If  $b = b'$ ,  $\mathcal{A}$  wins.



Adversary  $\mathcal{A}$

for  $i \in \text{poly}(n)$

for  $i \in \text{poly}(n)$

$$\forall \text{ adversaries } \mathcal{A}, \quad \Pr[\mathcal{A} \text{ wins game}] \leq \frac{1}{2} + \text{negligible}$$

# IND-CCA1 secure

Announcements

Introduction

Objectives

Symmetric Key  
Encryption

Ciphertext IND

IND-KPA

IND-CPA

**IND-CCA1**

IND-CCA2

Achieve IND-CPA

One Time Pad

AES Block Cipher

Summary



Challenger  $\mathcal{C}$



Adversary  $\mathcal{A}$

*Phases*

*setup*

$k \leftarrow \text{Gen}(1^n)$

*decrypt ciphertext and*

*encrypt plaintext*

$m_i \leftarrow \text{Dec}(k, c_i)$

$c_j \leftarrow \text{Enc}(k, m_j)$

*challenge cipher*

$b \xleftarrow{\$} \{0, 1\}$

$c^* \leftarrow \text{Enc}(k, m_b^*)$

*encrypt plaintext*

$c'_j \leftarrow \text{Enc}(k, m'_j)$

*send bit*

*determine win*

If  $b = b'$ ,  $\mathcal{A}$  wins.

$c_i, m_j$

for  $i, j \in \text{poly}(n)$

$m_i, c_j$

$m_0^*, m_1^*$

$c^*$

$m'_j$

for  $j \in \text{poly}(n)$

$c'_j$

$b'$

# IND-CCA1 secure

Announcements

Introduction

Objectives

Symmetric Key  
Encryption

Ciphertext IND

IND-KPA

IND-CPA

**IND-CCA1**

IND-CCA2

Achieve IND-CPA

One Time Pad

AES Block Cipher

Summary



*Phases*

*setup*

*decrypt ciphertext and*

*encrypt plaintext*

*challenge cipher*

*encrypt plaintext*

*send bit*

*determine win*

Challenger  $\mathcal{C}$

$k \leftarrow \text{Gen}(1^n)$

$m_i \leftarrow \text{Dec}(k, c_i)$

$c_j \leftarrow \text{Enc}(k, m_j)$

$b \xleftarrow{\$} \{0, 1\}$

$c^* \leftarrow \text{Enc}(k, m_b^*)$

$c'_j \leftarrow \text{Enc}(k, m'_j)$

If  $b = b'$ ,  $\mathcal{A}$  wins.

Adversary  $\mathcal{A}$

for  $i, j \in \text{poly}(n)$

for  $j \in \text{poly}(n)$

$c_i, m_j$

$m_i, c_j$

$m_0^*, m_1^*$

$c^*$

$m'_j$

$c'_j$

$b'$

$$\forall \text{ adversaries } \mathcal{A}, \quad \Pr[\mathcal{A} \text{ wins game}] \leq \frac{1}{2} + \text{negligible}$$

# IND-CCA2 secure



*Phases*

Challenger  $\mathcal{C}$

Adversary  $\mathcal{A}$

*setup*

$k \leftarrow \text{Gen}(1^n)$

*decrypt ciphertext and*

*encrypt plaintext*

$m_i \leftarrow \text{Dec}(k, c_i)$

$c_j \leftarrow \text{Enc}(k, m_j)$

*challenge cipher*

$b \xleftarrow{\$} \{0, 1\}$

$c^* \leftarrow \text{Enc}(k, m_b^*)$

*decrypt ciphertext and*

*encrypt plaintext*

$m'_i \leftarrow \text{Dec}(k, c'_i)$

$c'_j \leftarrow \text{Enc}(k, m'_j)$

*send bit*

*determine win*

If  $b = b'$ ,  $\mathcal{A}$  wins.

$c_i, m_j$

←

for  $i, j \in \text{poly}(n)$

$m_i, c_j$

→

$m_0^*, m_1^*$

←

$c^*$

→

$c'_i, m'_j$

←

for  $i, j \in \text{poly}(n)$ , where  $c'_i \neq c^*$

$m'_i, c'_j$

→

$b'$

←

Announcements

Introduction

Objectives

Symmetric Key  
Encryption

Ciphertext IND

IND-KPA

IND-CPA

IND-CCA1

**IND-CCA2**

Achieve IND-CPA

One Time Pad

AES Block Cipher

Summary

# IND-CCA2 secure



*Phases*

Challenger  $C$

Adversary  $\mathcal{A}$

*setup*

$k \leftarrow \mathbf{Gen}(1^n)$

*decrypt ciphertext and*

*encrypt plaintext*

$m_i \leftarrow \mathbf{Dec}(k, c_i)$

$c_j \leftarrow \mathbf{Enc}(k, m_j)$

*challenge cipher*

$b \xleftarrow{\$} \{0, 1\}$

$c^* \leftarrow \mathbf{Enc}(k, m_b^*)$

*decrypt ciphertext and*

*encrypt plaintext*

$m'_i \leftarrow \mathbf{Dec}(k, c'_i)$

$c'_j \leftarrow \mathbf{Enc}(k, m'_j)$

*send bit*

*determine win*

If  $b = b'$ ,  $\mathcal{A}$  wins.

$\xleftarrow{c_i, m_j}$

for  $i, j \in \text{poly}(n)$

$\xrightarrow{m_i, c_j}$

$\xleftarrow{m_0^*, m_1^*}$

$\xrightarrow{c^*}$

$\xleftarrow{c'_i, m'_j}$

for  $i, j \in \text{poly}(n)$ , where  $c'_i \neq c^*$

$\xrightarrow{m'_i, c'_j}$

$\xleftarrow{b'}$

$$\forall \text{ adversaries } \mathcal{A}, \quad \Pr[\mathcal{A} \text{ wins game}] \leq \frac{1}{2} + \text{negligible}$$

Announcements

Introduction

Objectives

Symmetric Key

Encryption

Ciphertext IND

IND-KPA

IND-CPA

IND-CCA1

IND-CCA2

Achieve IND-CPA

One Time Pad

AES Block Cipher

Summary

# How are these security definitions related?

IND-CCA2 secure  $\implies$  IND-CCA1 secure  
 $\implies$  IND-CPA secure  $\implies$  IND-KPA secure

This means that IND-CCA2 is the stronger security definition.  
In cryptography we want the **strongest** security to hold.

Example: If your protocol is IND-CCA1 secure, then it is IND-CPA and IND-KPA secure. However, it is not necessarily IND-CCA2 secure.

Announcements

Introduction

Objectives

Symmetric Key  
Encryption

Ciphertext IND

IND-KPA

IND-CPA

IND-CCA1

IND-CCA2

Achieve IND-CPA

One Time Pad

AES Block Cipher

Summary

# How are these security definitions related?

Announcements

Introduction

Objectives

Symmetric Key  
Encryption

Ciphertext IND

IND-KPA

IND-CPA

IND-CCA1

**IND-CCA2**

Achieve IND-CPA

One Time Pad

AES Block Cipher

Summary

IND-CCA2 insecure  $\Leftarrow$  IND-CCA1 insecure  
 $\Leftarrow$  IND-CPA insecure  $\Leftarrow$  IND-KPA insecure

Example: If your protocol is IND-CCA1 insecure, then it is IND-CCA2 insecure. However, it is not necessarily IND-CPA or IND-KPA insecure.

# Note

Announcements

Introduction

Objectives

Symmetric Key  
Encryption

Ciphertext IND

IND-KPA

IND-CPA

IND-CCA1

IND-CCA2

Achieve IND-CPA

One Time Pad

AES Block Cipher

Summary

In each security definition, we must be secure against all possible adversaries that are allowed to behave within the limits of the definition.

For instance, in IND-KPA the adversary will not receive answers to any encryption queries. (*Note that “encrypt plaintext” phase is in IND-CPA, but not in IND-KPA.*)



# Achieve IND-CPA

Announcements

Introduction

Objectives

Symmetric Key  
Encryption

Ciphertext IND

IND-KPA

IND-CPA

IND-CCA1

IND-CCA2

Achieve IND-CPA

One Time Pad

AES Block Cipher

Summary

Let's set a reasonable security goal. For the scope of this class, we want a symmetric encryption scheme that is IND-CPA.

# Let's build something! (*"move fast and break things", right?*)

Announcements

Introduction

Objectives

Symmetric Key  
Encryption

Ciphertext IND

IND-KPA

IND-CPA

IND-CCA1

IND-CCA2

Achieve IND-CPA

**One Time Pad**

AES Block Cipher

Summary



We're familiar with XOR.

A	B	$A \oplus B$
0	0	0
0	1	1
1	0	1
1	1	0

The output of two random inputs XORed is 0 w.p.  $1/2$  and 1 w.p.  $1/2$ . This hides information!

# One Time Pad (OTP)

Let  $m$  be some  $n$  bit message or plaintext. OTP will sample a key  $k$  as some arbitrary  $n$  bit binary string.

$$\mathbf{Gen}(1^n) : \quad k \xleftarrow{\$} \{0, 1\}^n$$

Then OTP will produce an  $n$  bit ciphertext by XORing the message  $m$  with the key  $k$ .

$$\mathbf{Enc}(k, m) : \quad m \oplus k$$

$$\mathbf{Dec}(k, c) : \quad c \oplus k$$

Announcements

Introduction

Objectives

Symmetric Key

Encryption

Ciphertext IND

IND-KPA

IND-CPA

IND-CCA1

IND-CCA2

Achieve IND-CPA

One Time Pad

AES Block Cipher

Summary

# Is OTP correct?

Announcements

Introduction

Objectives

Symmetric Key

Encryption

Ciphertext IND

IND-KPA

IND-CPA

IND-CCA1

IND-CCA2

Achieve IND-CPA

One Time Pad

AES Block Cipher

Summary

$$\mathbf{Gen}(1^n) : \quad k \xleftarrow{\$} \{0, 1\}^n$$

$$\mathbf{Enc}(k, m) : \quad m \oplus k$$

$$\mathbf{Dec}(k, c) : \quad c \oplus k$$

We have that  $\forall m$  messages of length  $n$ ,

$$\mathbf{Dec}(k, \mathbf{Enc}(k, m)) = \mathbf{Enc}(k, m) \oplus k = (m \oplus k) \oplus k = m \oplus (k \oplus k) = m \oplus 0^n = m.$$

We're done, right? Let's slow down. We should check which security definitions OTP satisfies.

# Is OTP IND-CPA? (*Break time~*)

Announcements

Introduction

Objectives

Symmetric Key  
Encryption

Ciphertext IND

IND-KPA

IND-CPA

IND-CCA1

IND-CCA2

Achieve IND-CPA

**One Time Pad**

AES Block Cipher

Summary

Let's slow down, take a break! Pass messages to your neighbor.

No idea what to talk about? Well, is OTP IND-CPA?

# Is OTP IND-CPA?

No. There  $\exists$  adversary  $\mathcal{A}$  with the following strategy:

Phases	Challenger $\mathcal{C}$		Adversary $\mathcal{A}$
<i>setup</i>	$k \xleftarrow{\$} \{0, 1\}^n$		
<i>encrypt plaintext</i>		$0^n = \underbrace{0 \dots 0}_{n \text{ times}}$ $\xleftarrow{\hspace{1.5cm}}$ $c$ $\xrightarrow{\hspace{1.5cm}}$	$k = c$
<i>challenge cipher</i>	$c = 0^n \oplus k$  $b \xleftarrow{\$} \{0, 1\}$  $c^* = m_b \oplus k$	$\xleftarrow{\hspace{1.5cm}} m_0, m_1$  $\xrightarrow{\hspace{1.5cm}} c^*$	Choose $m_0 \neq m_1$  If $c^* \oplus k = m_0$ , let $b' = 0$ . Otherwise, $b' = 1$ .
<i>encrypt plaintext</i>			
<i>send bit</i>		$\xleftarrow{\hspace{1.5cm}} b'$	
<i>determine win</i>	If $b = b'$ , $\mathcal{A}$ wins.		

Announcements

Introduction

Objectives

Symmetric Key  
Encryption

Ciphertext IND  
IND-KPA  
IND-CPA  
IND-CCA1  
IND-CCA2

Achieve IND-CPA

One Time Pad

AES Block Cipher

Summary

# Is OTP IND-CPA?

No. There  $\exists$  adversary  $\mathcal{A}$  with the following strategy:

Announcements

Introduction

Objectives

Symmetric Key  
Encryption

Ciphertext IND

IND-KPA

IND-CPA

IND-CCA1

IND-CCA2

Achieve IND-CPA

One Time Pad

AES Block Cipher

Summary

*Phases*

Challenger  $\mathcal{C}$

Adversary  $\mathcal{A}$

*setup*

$k \xleftarrow{\$} \{0, 1\}^n$

$0^n = \underbrace{0 \dots 0}_{n \text{ times}}$

*encrypt plaintext*

$c = 0^n \oplus k$

$\leftarrow$

$c$

$\longrightarrow$

$k = c$

*challenge cipher*

$m_0, m_1$

$\leftarrow$

Choose  $m_0 \neq m_1$

$b \xleftarrow{\$} \{0, 1\}$

$c^* = m_b \oplus k$

$c^*$

$\longrightarrow$

If  $c^* \oplus k = m_0$ , let  $b' = 0$ .

Otherwise,  $b' = 1$ .

*send bit*

$b'$

$\leftarrow$

*determine win*

If  $b = b'$ ,  $\mathcal{A}$  wins.

Since  $\mathcal{A}$  has the key  $k$ ,  $\mathcal{A}$  can just decrypt the challenge cipher, winning the game w.p. 1.

# Is OTP “secure”? *(No games. Intuition only, please!)*

Announcements

Introduction

Objectives

Symmetric Key  
Encryption

Ciphertext IND

IND-KPA

IND-CPA

IND-CCA1

IND-CCA2

Achieve IND-CPA

One Time Pad

AES Block Cipher

Summary

If you encrypt two messages with the same key, then you leak crucial information.

For example, let  $m_1$  and  $m_2$  be any two messages encrypted with key  $k$ . If an adversary got hold of the encryptions  $c_1 = m_1 \oplus k$  and  $c_2 = m_2 \oplus k$ , then they could calculate  $c_1 \oplus c_2 = m_1 \oplus k \oplus m_2 \oplus k = m_1 \oplus m_2$ .

This leaks information about the messages!



# Is OTP “secure”?

Announcements

Introduction

Objectives

Symmetric Key  
Encryption

Ciphertext IND

IND-KPA

IND-CPA

IND-CCA1

IND-CCA2

Achieve IND-CPA

**One Time Pad**

AES Block Cipher

Summary

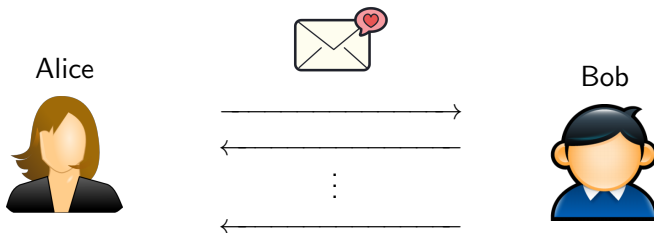
Historically, OTP was still used. Why?

It's use case is hinted in its name. **One Time** Pad. A key should only be used once. The key should be changed each time a message is encrypted.

If you don't reuse the key for multiple messages, OTP can be considered secure.

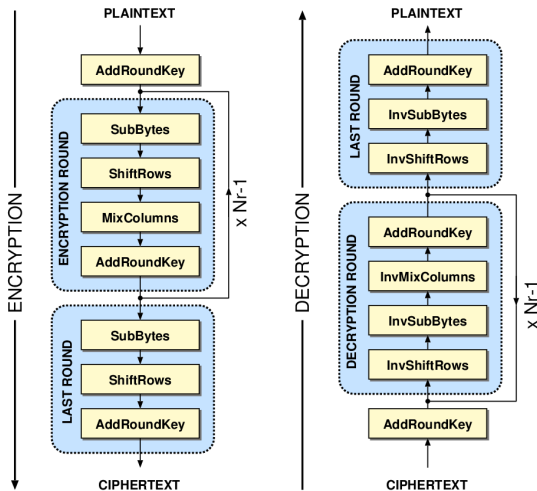
# Downsides to OTP

- Not IND-CPA
- No key reuse
  - can't reuse the key for multiple messages
- Key length must be message length
  - can only encrypt messages of the same length  $n$  as the key



Being optimistic that Bob will reply back to Alice, this scheme is rather impractical for our purpose.

For comparison, here's one building block...



...of an encryption construction.

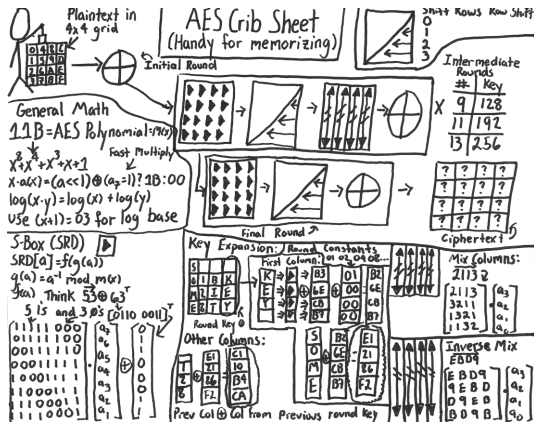
AES Block Cipher

- 128 or 192 or 256 bit key
- up to 14 cycles of repetition

This is complex!  
We don't expect you to understand how it works.

# AES block cipher

If you're curious...



...check out "AES stick figure" online.

# Is AES “secure”?

Announcements

Introduction

Objectives

Symmetric Key

Encryption

Ciphertext IND

IND-KPA

IND-CPA

IND-CCA1

IND-CCA2

Achieve IND-CPA

One Time Pad

AES Block Cipher

Summary

While many attacks have been presented, some were found to be faulty or impractical against the full protocol. As such, AES is **believed** to be secure in practice.

Where's the proof?

*(Correct response: Which security definition? IND-CPA)*

Actually, turns out that AES is not **proven** to be secure.

Fun fact: If we had a real world encryption construction that was provably secure, then  $P \neq NP$ !

# AES in the real world

Announcements

Introduction

Objectives

Symmetric Key  
Encryption

Ciphertext IND

IND-KPA

IND-CPA

IND-CCA1

IND-CCA2

Achieve IND-CPA

One Time Pad

AES Block Cipher

Summary

- Two Belgian cryptographers (Vincent Rijmen, Joan Daemen) constructed this scheme which won the AES encryption competition
  - Henceforth to be known as AES
- US Government standard
  - AES is standardized as Federal Information Processing Standard 197 (FIPS 197) by NIST
- Industry
  - SSL/TLS
  - SSH
  - WinZip
  - BitLocker
  - Mozilla Thunderbird
  - Skype

# Moral of the day

~~“Move fast and break things”~~

Put well reasoned thought into how you build secure systems.  
Use established cryptographic protocols and primitives.

Don't build your own cryptography using only knowledge  
learned from this class and its prerequisite classes!

Announcements

Introduction

Objectives

Symmetric Key  
Encryption

Ciphertext IND

IND-KPA

IND-CPA

IND-CCA1

IND-CCA2

Achieve IND-CPA

One Time Pad

AES Block Cipher

Summary

# Let's take our time...

Announcements

Introduction

Objectives

Symmetric Key  
Encryption

Ciphertext IND

IND-KPA

IND-CPA

IND-CCA1

IND-CCA2

Achieve IND-CPA

One Time Pad

**AES Block Cipher**

Summary

...next time to look into block ciphers and how we can chain them to achieve IND-CPA.



# Alice learned today that ...

- confidentiality can be achieved using cryptographic encryption
  - we'll focus on symmetric key
  - we'll see asymmetric key later
- security definitions can be phrased as adversarial games
  - we'll focus on achieving IND-CPA secure encryption
- constructing real-world cryptography relies on these theoretical definitions
  - OTP is not IND-CPA since it's deterministic
  - AES block cipher is quite complicated and is built off of some block cipher definition which we will see tomorrow

Announcements

Introduction

Objectives

Symmetric Key  
Encryption

Ciphertext IND

IND-KPA

IND-CPA

IND-CCA1

IND-CCA2

Achieve IND-CPA

One Time Pad

AES Block Cipher

Summary