Introduction to Cryptography

Definitions and Common Terminology

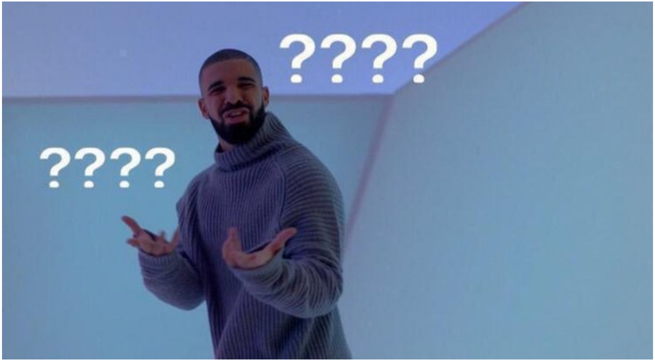
Based on 1.1 of Schneier's *Applied Cryptography*

Lecture notes of Alexander Wood
awood@jjay.cuny.edu

John Jay College of Criminal Justice

What is cryptography?

Spend a few minutes thinking about how you would define this term.



What is cryptography?

Hopefully we have focused in on the main ideas:

What is cryptography?

Hopefully we have focused in on the main ideas:

- *Communication* between two (or more) parties..

What is cryptography?

Hopefully we have focused in on the main ideas:

- *Communication* between two (or more) parties..
- .. which is *secure* ...

What is cryptography?

Hopefully we have focused in on the main ideas:

- *Communication* between two (or more) parties..
- .. which is *secure* ...
- ... in the presence of *adversaries*.

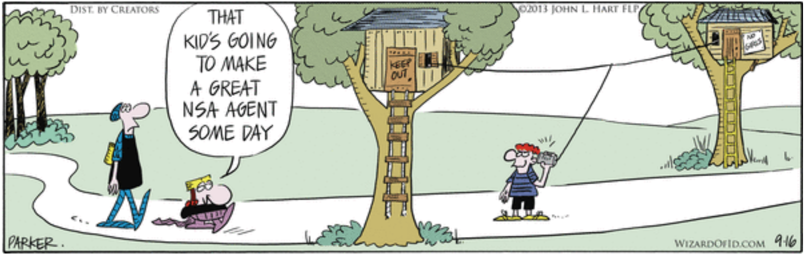
What is Cryptography?

Cryptography is secure communication between two or more parties in the presence of adversaries.

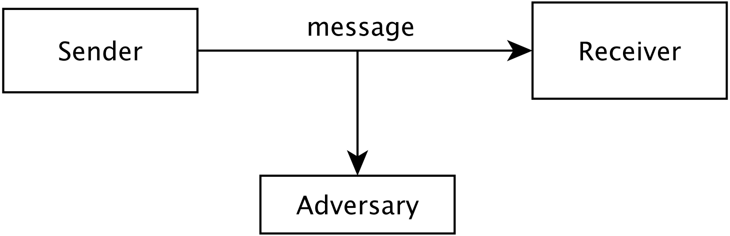
Who are the players?

- The **sender** wishes to send a message.
- The **receiver** is the intended recepient of the message.
- The **adversary** is a malicious third party who wishes to obtain (at least partial) information about the message.

The Basic Setup

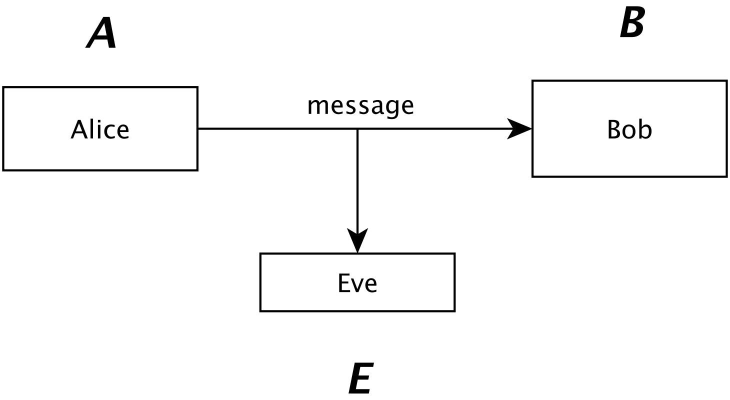


The Basic Setup

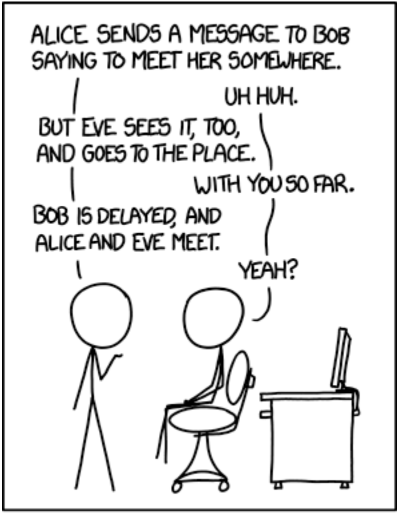


Let’s give names to our players.

The Basic Setup

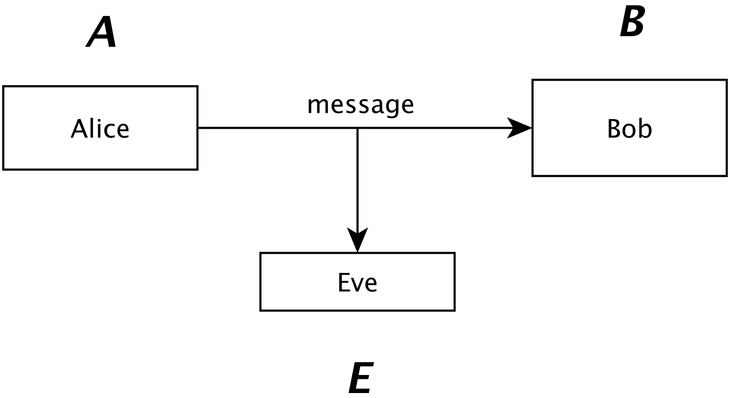


Alice, Bob, and Eve


ALICE SENDS A MESSAGE TO BOB SAYING TO MEET HER SOMEWHERE.
UH HUH.
BUT EVE SEES IT, TOO, AND GOES TO THE PLACE.
WITH YOU SO FAR.
BOB IS DELAYED, AND ALICE AND EVE MEET.
YEAH?

I'VE DISCOVERED A WAY TO GET COMPUTER SCIENTISTS TO LISTEN TO ANY BORING STORY.

The Basic Setup

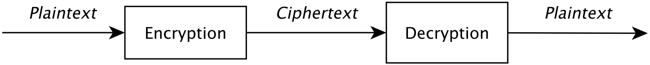


Observe that we have not yet introduced any way of *encrypting* the message.

Messages & Encryption

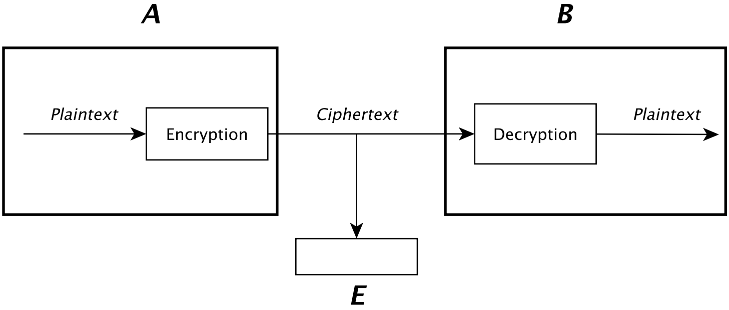
- The message is originally in **plaintext**, which can be plainly read.
- We hide the substance of the message using **encryption**, which yields a disguised message, or **ciphertext.**
- Turning the ciphertext back into plaintext is called **decryption.**

Encyption and Decryption



An example scenario

Alice must encrypt the message, and Bob must decrypt it.



Note now that if Eve intercepts the message, she receives only the ciphertext.

Sounding Like Cryptologists (AKA, some terminology)

- **Cryptography** is the science of secure communication between multiple parties, and it is practiced by **cryptographers**.
- **Cryptanalysis** is science of breaking ciphertext and is practiced by **cryptanalysts**.
- Cryptography *and* cryptanalysis is **cryptology** and its practitioners are **cryptologists**.

Naming Conventions

- M is the plaintext message
- C is the ciphertext, or the encrypted plaintext.
- E or $Enc()$ represents encryption, where

$$Enc(M) = C$$

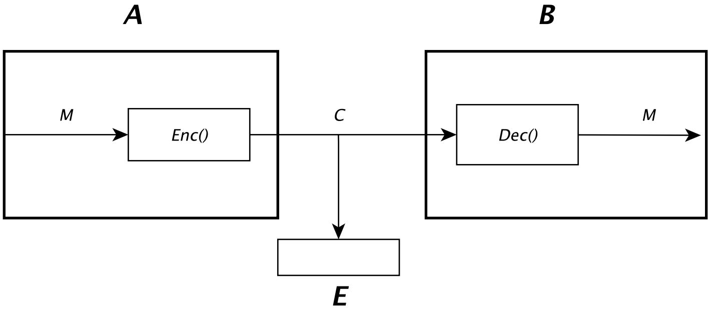
- D or $Dec()$ represents decryption, where

$$Dec(C) = M$$

We should be able to encrypt then decrypt the message to recover the original message:

$$Dec(Enc(M)) = M$$

Our super cool diagram



But really, what’s in a message?

A plaintext message *M* can be...

- A stream of bits
- a text file
- a digitized voice stream
- a video

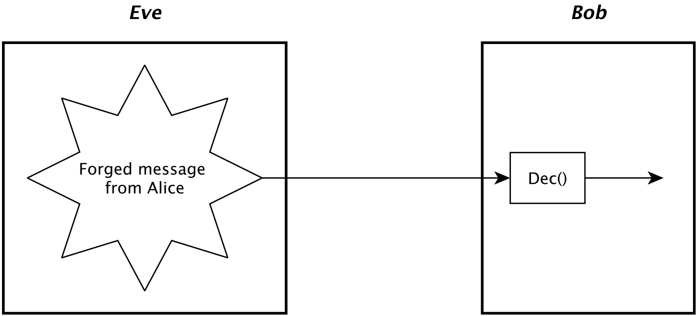
The ciphertext *C*, or encryption of the message, is binary data. It may be larger or smaller (if compressed – discussed later in course) than the original message.

What else do we want from our cryptographic protocols?

- Authentication
- Integrity
- Nonrepudiation

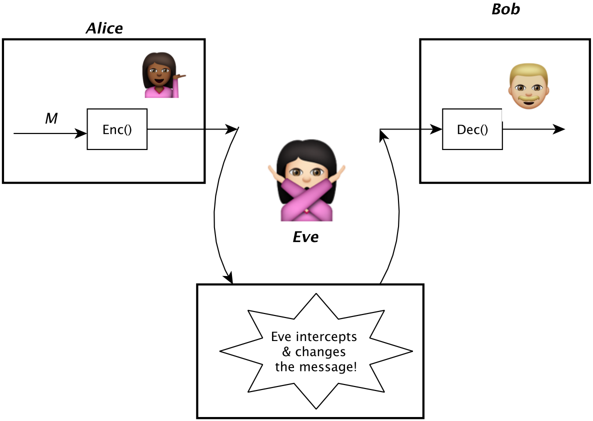
Authentication

A third party should not be able to send a message as someone else. In other words, the receiver of a message should be able to accurately determine its origin, or authenticity.



Integrity

The receiver should be able to verify that a message was not modified after being sent.



Nonrepudiation

The sender of a message cannot falsely claim to have not sent it.

I NEVER SAID THAT. I DIDN'T SAY THAT. WHERE DID YOU FIND THIS?
I NEVER SAID THAT EITHER.

Ciphers

A **cryptographic algorithm** is also called a **cipher.** It consists of mathematical functions for encryption and for decryption.

I got the keys

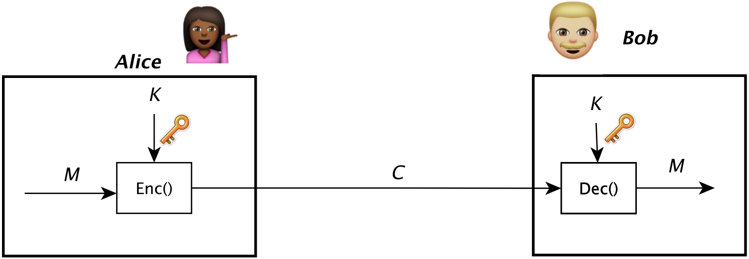
Keys

Modern cryptography uses a **key** K, taken from a possible range of values called the **keyspace**, for encryption and decyption algorithms. Common notation for encryption and decryption under a key K is given by use of a subscript:

$$E_K(M) = C$$

$$D_K(C) = M$$

Keys



Keys

The encryption key K and decryption key $\bar{K}$ are sometimes different.

$$E_K(M) = C$$

$$D_{\bar{K}}(C) = M$$

Cryptosystem

The term **cryptosystem** describes the encryption and decryption algorithms, as well as all possible plaintexts, ciphertexts, and keys.

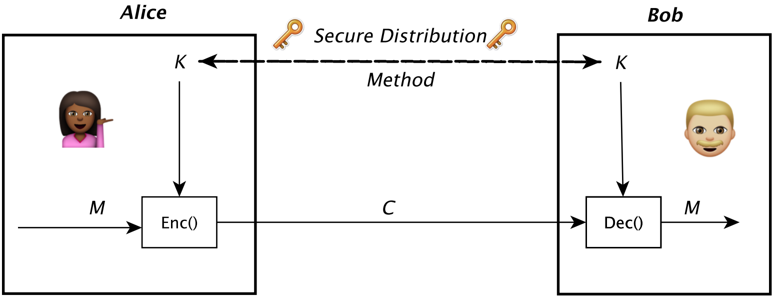
Public versus Private

There are two main types of algorithms used in cryptosystems

- **Private-key**, or **symmetric** algorithms
- **Public-key**, or **asymmetric** algorithms

Symmetric Encryption

These were the first types of encryption algorithms created! The encyption and decryption keys are usually the same, and they must be agreed upon *beforehand* by all involved parties.



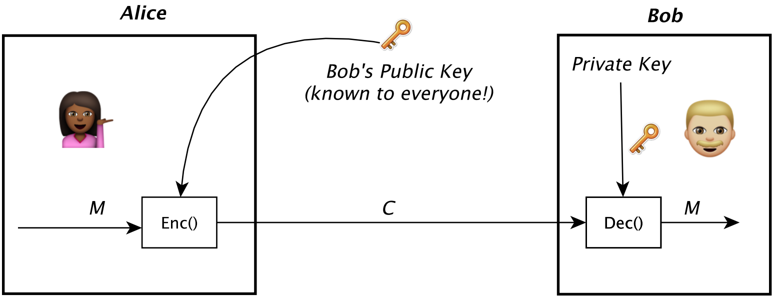
Public Key Encryption

Revolutionized by the publication of Diffie-Hellman Key Exchange in 1974. In asymmetric or public key schemes, it is not necessary to agree on a key beforehand.

Public Key Encryption

Now, Bob has both a public key, which he shares publicly, and a private key, which he tells no one. Anyone can send Bob and encrypted message using his public key, but only Bob can decrypt it.

Public Key Encryption



First, Bob publishes his public key. Then, Alice encrypts a plaintext message using this public key and sends it to Bob. Bob uses his private key and the decryption algorithm to decrypt the message.

Cryptanalysis

Cryptanalysis is the attempt to recover an encrypted message without access to the key, and to find weaknesses in the cryptosystem. Call an attemped cryptanalysis an **attack** on the cryptosystem.

Kerckhoffs' Principle

In the 1880s, Dutch mathematician Kerckhoff published several design principles for cryptographic algorithms.

One of these, which we still follow to this day, states that even an adversary who has all of the information about how your cryptosystem operates, but does not have the private keys, will not be able to break your cryptosystem.

In other words, *we should be able to publish all of the information about how the cryptosystem works without compromising its security.*

Cryptanalytic Attacks

There are many!

- Ciphertext-Only Attack
- Known-Plaintext Attack
- Chosen-Plaintext Attack
- Adaptive-Chosen-Plaintext Attack
- Chosen-Ciphertext Attack
- Rubber-hose Cryptanalysis

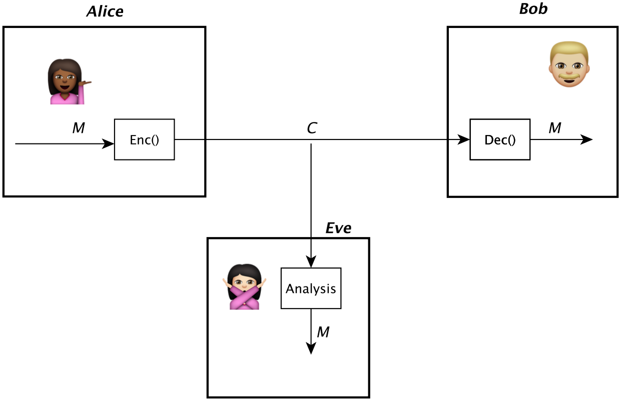
Ciphertext-Only Attacks

- *Given*: Ciphertexts $C_1, C_2, \ldots, C_k$
- *Deduce:* $M_1, M_2, \ldots, M_k$ or *Enc*().

The cryptanalyst Eve eavesdropped on communication between Alice and Bob and has the ciphertext of several messages. She attempts to use properties of these plaintexts to deduce either the contents of the messages, the keys, or both.

Ciphertext-Only Attacks

Eve determines they key(s) or the plaintext(s) by analyzing intercepted ciphertexts.

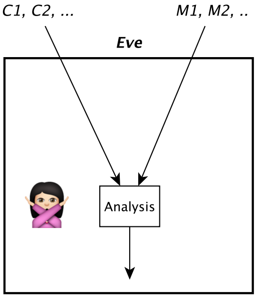


Known-Plaintext Attack

- *Given:* Plaintexts and their associated ciphertexts
- *Deduce:* Keys and/or a method of deducing plaintexts from ciphertexts

  Now, Eve not only as access to the ciphertext of several messages, but also their corresponding plaintexts. She must deduce the key(s) to the algorithm, or a method of obtaining the plaintexts from ciphertexts.

Known-Plaintext Attack

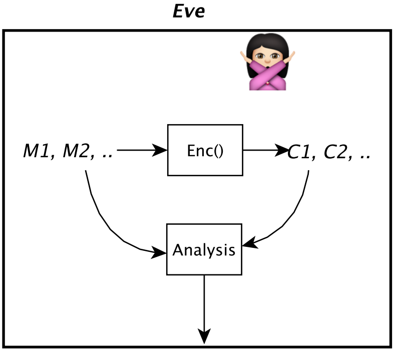


Eve deduces information about the cryptosytem using intercepted ciphertexts and their corresponding plaintexts.

Chosen-Plaintext Attack

Eve has access to plaintexts and their corresponding ciphertexts, as before. However in a chosen-plaintext attack, Eve gets to choose which plaintexts to encrypt!

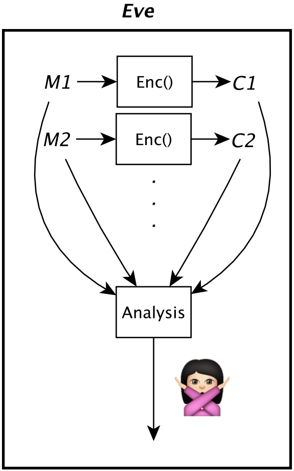
Chosen plaintext attack



Eve chooses which plaintexts to encrypt.

What happens if a public-key cryptosystem is vulnerable to this attack?

Adaptive-Chosen-Plaintext Attack



This is similar to the previous attack. However, before, Eve had to choose all of the plaintexts she would like to encrypt up front. Now, Eve can adapt the plaintexts she encrypts based off of previous encryptions.

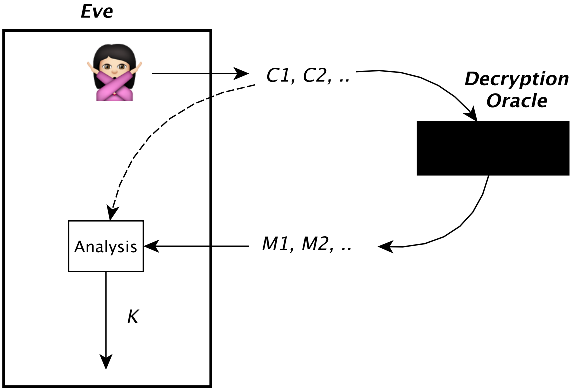
What happens if a public-key cryptosystem is vulnerable to this attack?

Chosen Ciphertext Attack

- *Given:* $C_1, M_1 = D_K(C_1), \ldots, M_i = D_K(C_i)$
- *Deduce:* K

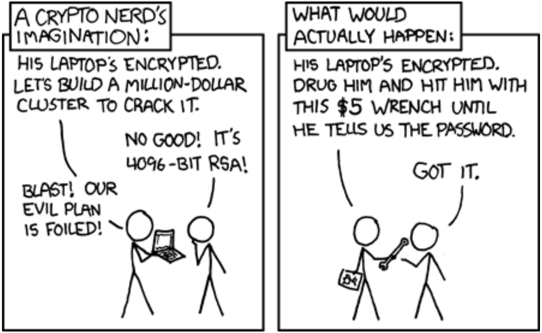
This attack is most relevant for public-key encryption. Eve can choose any ciphertexts to be decrypted, and is able to access their decrypted plaintexts.

Chosen Ciphertext Attack



Rubber Hose Cryptanalysis

Threaten/blackmail/torture the keyholder until they give you the key.


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

https://xkcd.com/538/

Security

There are many ways to define security. The definition of security we use must correspond to the cryptosystem we are using, as well as the context in which we use that scheme.

What do you think are some of the key points that must be addressed by a definiton of security?

Security

It should be impossible for the attacker to...

- ...recover the key..
- ...recover the entire plaintext from the ciphertext...
- ...recover part of the plaintext from the cipher text, and
- the ciphertext leaks no additional information about the underlying plaintext.

These are still not precisely defined terms. We will see various definitions of security throughout the course.

(From *Introduction to Modern Cryptography* by Katz & Lindell)

Security

You are probably safe if...

- ... the cost of breaking an algorithm is greater than the value of the encrypted data...
- ... or if the time it would take to break the algorithm is longer than then amount of time the data must remain secret.

We will see definitions of security later in the course built around these concepts.

Unconditional Security

We call an algorithm unconditionally secure if no amount of time and/or computational power would be enough for any adversary to ever recover the plaintext. The only unconditionally secure cryptosystem is the **one-time pad** which we will see later in this course.

Brute-Force Attacks

All other cryptosystems could be broken by a ciphertext-only attack. The attacker would simply have to try every possible key until she found the correct one. This is called a **brute-force attack.**

A cryptosystem is called **computationally secure** if it is unfeasible to break the system with current and foreseeable future computational resources.

Example From Textbook

If an algorithm has a processing complexity of 2^{128}, then 2^{128} operations are required to break the algorithm. (These operations may be complex and time-consuming.) Still, if you assume that you have enough computing speed to perform a million operations every second and you set a million parallel processors against the task, it will still take over 10^{19} years to recover the key. That's a billion times the age of the universe.