



Cryptography

Theory Club Workshop 4

Daniel Hathcock

Overview

Goals of cryptography,
types of cryptography.

01

Private-key Crypto

Exchanging messages with a
shared private key.

02

Message Authentication

Verifying message integrity and
sender identity.

03

TABLE OF CONTENTS

04

Public-key crypto

Exchange information without a
shared key

05

Miscellaneous Crypto

Secret sharing, interactive proof
systems, secure multiparty
computation.

01

Overview



Goals of Cryptography



Hide information


How can you prevent an adversary from gaining secret information?

Share information

How can you exchange information with trusted parties?

Tractability

Schemes should be able to be implemented under reasonable time and space constraints.



Provable Security

How do you convince someone of your identity / knowledge without revealing any information about yourself?

Types of Cryptography

Private Key

Send a secret message using a shared secret key

Public Key

Send a secret message using a public/private key pair

Hashing

Compute a one-way function

Authentication

Verify message integrity and authenticity

Zero-Knowledge Proofs

Share knowledge without revealing too much information

Secret Sharing

Split a key into parts so that if any n are present, the key can be reconstructed





Cryptographic Assumptions

“The cipher method must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience.”

Kerckhoff's Principle

How much power does the adversary have?

- Unlimited power (information theoretic security)
- Probabilistic polynomial time

Models of Security



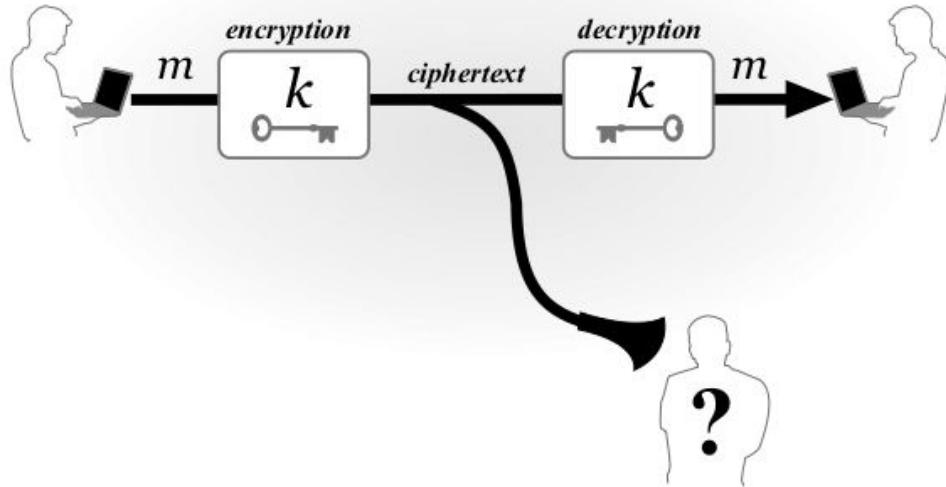


02

PRIVATE KEY

You can enter here the subtitle if you need it

Private Key Cryptography



- Alice and Bob share a private key k .
- Alice wants to send a secret message m to Bob over a public channel.
- Idea: use a scheme which *encrypts* the message into a ciphertext c using k , then allows for the decryption back into m .

Questions:

- How large can keys and messages be?
- What type of security do we want?
- What can we assume about the adversary?

One Time Pad

Suppose the message is a bitstring in $\{0,1\}^n$. We allow the key to be any length (can depend on the message length), and suppose Alice and Bob can generate the key ahead of time through any means necessary.

Question: Can you design a scheme which achieves “perfect security”?

ENCRYPT

$$\begin{array}{r} \oplus \\ \begin{array}{r} \mathbf{00110101} \text{ Plaintext} \\ \mathbf{11100011} \text{ Secret Key} \\ \hline \mathbf{11010110} \text{ Ciphertext} \end{array} \end{array}$$

DECRYPT

$$\begin{array}{r} \oplus \\ \begin{array}{r} \mathbf{11010110} \text{ Ciphertext} \\ \mathbf{11100011} \text{ Secret Key} \\ \hline \mathbf{00110101} \text{ Plaintext} \end{array} \end{array}$$

03

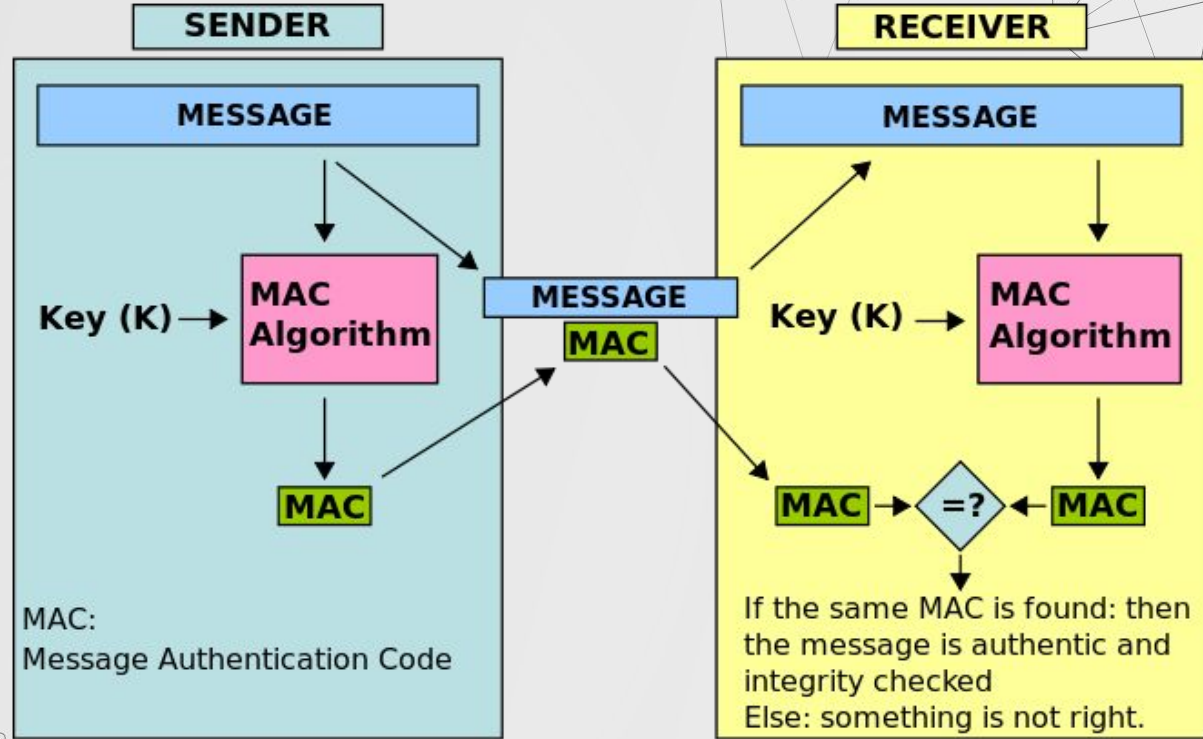
MESSAGE AUTHENTICATION

You can enter here the subtitle if you need it



Message Authentication

- Goals:
 - Verify sender identity
 - Ensure message integrity
- Alice and Bob share a secret key K .
- The message M is *not* secret.
- **Idea:** Hasing
 - Use a *keyed hashing function*.
 - If Eve changes the message, she would have to know the correct new hash.



04

PUBLIC KEY

We can share secrets over a public channel.

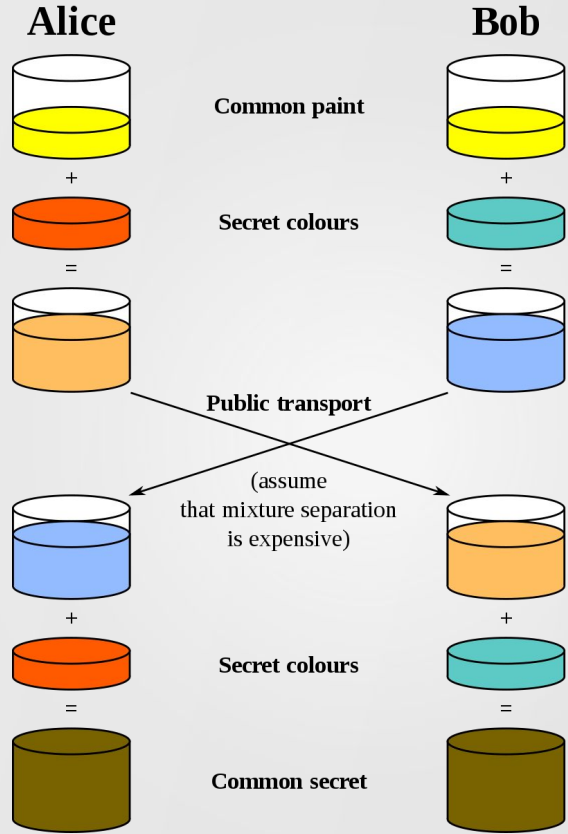


Public Key (Asymmetric) Crypto

- Sharing a key beforehand is bothersome.
- Is there a way to share a private key without meeting or trusting a channel/courier (key exchange)?
- Is there a way to send messages without ever exchanging a secret key?



Idea:



DIFFIE HELLMAN PROCEDURE



PUBLIC INFO

Choose **public modulus p** and **base g**



ALICE SENDS...

Alice chooses **secret number a**. Sends $A = g^a \bmod p$ to Bob.



BOB SENDS...

Bob chooses **secret number b**. Sends $B = g^b \bmod p$ to Alice



ALICE COMPUTES...

$$B^a \bmod p = (g^b)^a \bmod p$$



BOB COMPUTES...

$$A^b \bmod p = (g^a)^b \bmod p$$



FIN

Secrecy achieved: the secret number is $g^{ab} \bmod p$.

WHAT CAN EVE DO

She sees:

- g and p
- $g^a \pmod p$
- $g^b \pmod p$

She wants:

- $g^{(ab)} \pmod p$

Diffie Hellman Problem

She sees:

- g , p , and $g^a \pmod p$

She wants:

- a' such that $g^{(a')} = g^a \pmod p$

Discrete Log Problem

Problem: Prove that Diffie Hellman is no harder than discrete log.

Extra Challenge: Prove that Diffie Hellman is at least as hard as discrete log.



05

ZERO KNOWLEDGE

Prove something without revealing any new information

ZERO KNOWLEDGE PROOFS



COMPLETENESS

If the statement is true, the honest verifier (that is, one following the protocol properly) will be convinced of this fact by an honest prover.

If the statement is false, no cheating prover can convince the honest verifier that it is true, except with some small probability.

SOUNDNESS



ZERO KNOWLEDGE

If the statement is true, no verifier learns anything other than the fact that the statement is true. In other words, just knowing the statement (not the secret) is sufficient to imagine a scenario showing that the prover knows the secret.

RED & GREEN BALLS

“Imagine your friend is colour-blind and you have two balls: one red and one green, but otherwise identical. To your friend they seem completely identical and he is skeptical that they are actually distinguishable. You want to *prove to him they are in fact differently-coloured*, but nothing else, thus you do not reveal which one is the red and which is the green.”

K COLORINGS

Say Peggy has a graph G and some k coloring of it. How can Peggy prove she has a k coloring to Victor without revealing her k coloring?

Weird Question: What if Peggy didn't have a k -coloring but DID have a time machine that could rewind time by 10 minutes? How might she use that to trick Victor into thinking she does have a valid k -coloring?

DISCRETE LOG

“Peggy wants to prove to Victor that she knows the discrete log of a given value in a given group. [\[5\]](#)

For example, given a value y , a large prime p and a generator g , she wants to prove that she knows a value x such that $g^x \pmod{p} = y$, without revealing x .”

A background network diagram consisting of a complex web of interconnected nodes and lines. The nodes are represented by small black dots, and the lines are thin, light gray. The network is denser on the left side and becomes sparser towards the right. Some nodes are larger than others, and some lines are thicker, creating a sense of depth and connectivity.

05 + ϵ

SECRET SHARING

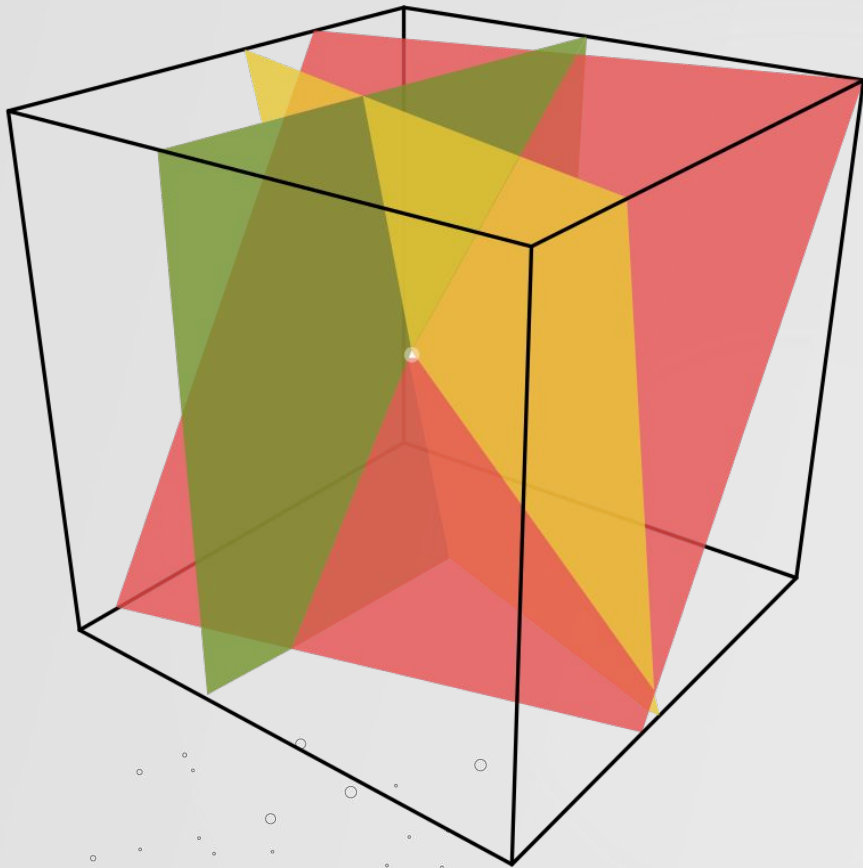
Among a group of people

PROBLEM DEFINITION

We have $m > n$ people. We want some subset of at least n people to be able to unlock the secret.

SECRET SHARING

A group of $n - 1$ people should fail in unlocking the secret.



ONE SOLUTION

Let your secret be expressed as a point in \mathbb{R}^n . Randomly generate m affine hyperplanes through your point. We may consider them to be in general position*. Note that n hyperplanes will intersect at exactly a point.

* A group of objects in general position is defined as a “probabilistically likely” configuration. For example n points in general position might be defined as “no three points on a line” since it is unlikely to get three random points exactly on a line.



THANKS

Does anyone have any questions?

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, and infographics & images by **Freepik**.

Please keep this slide for attribution.