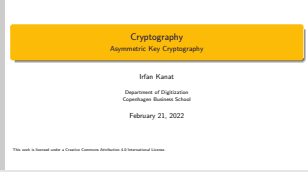
Cryptography

Asymmetric Key Cryptography

Irfan Kanat

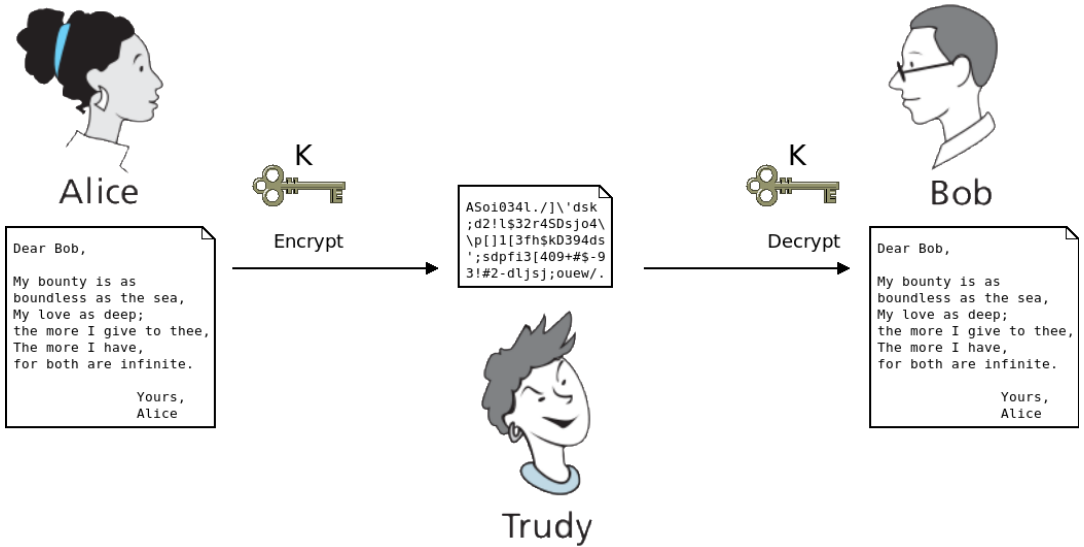
Department of Digitization
Copenhagen Business School

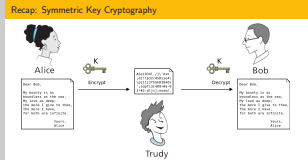
February 21, 2022



In this presentation we focus on asymmetric key cryptography and how it is used to ensure Confidentiality, Integrity, and Authentication.

Recap: Symmetric Key Cryptography





If Alice and Bob have met before and shared a key,
Then they can encrypt and decrypt their messages without Trudy getting any wiser.
A single key both locks and unlocks the box and reveals the tender words of our office lovers.

The Problem with Symmetric Key Cryptography

For two thousand years cryptography required a shared key.

This is ok if you can meet and exchange keys.

Did you exchange keys with your bank?

The Problem with Symmetric Key Cryptography
For two thousand years cryptography required a shared key.
This is ok if you can meet and exchange keys.
Did you exchange keys with your bank?

Symmetric Key cryptography is perfectly fine if you can share keys with the other party.
Yet there are so many use cases where we need to communicate with parties that we won't meet. An example was submarines leaving for months long voyages during world war II. For other troops that were part of the network, new keys could be sent via courier. The submarines had to store keys in advance. This made them a target.
A less exciting but still more relevant case is websites. You often see the green lock icon in the address bar. Indicating you are communicating with the right party and your communications are secured. But you have not exchanged keys with every web site in the world...
How come you can tell you are talking to your bank and not some scammers? How come you can be sure your information is encrypted?

Big Idea: Securing Data in Transit

Alice and Bob want to communicate securely

- Confidentiality
- Integrity
- Authentication

Big Idea: Securing Data in Transit
Alice and Bob want to communicate securely
- Confidentiality
- Integrity
- Authentication

It is fine to encrypt and decrypt the data with a single key if that data is sitting on your devices, when you want to exchange data through an unreliable medium (such as internet) you need to consider a few things.
Principles of secure communications.
AGAIN CIA but a different A this time.
Confidentiality: That Trudy can not read your love letters.
Integrity: That Trudy can not alter your love letters.
Authentication: That Trudy can not pretend to be Alice.

Asymmetric Key Cryptography

We shared keys for 2000 years

Asymmetric Key Cryptography
We shared keys for 2000 years

Asymmetric Key Cryptography

We shared keys for 2000 years

Then we found a better way!

Asymmetric Key Cryptography
We shared keys for 2000 years
Then we found a better way!


Asymmetric Key Cryptography

We shared keys for 2000 years

Then we found a better way!

RADICALLY DIFFERENT!

MARVELOUSLY ELEGANT!

Asymmetric Key Cryptography
We shared keys for 2000 years
Then we found a better way!
RADICALLY DIFFERENT!
MARVELOUSLY ELEGANT!

Sharing keys is so 1970.

In 76, we found a better idea.

Asymmetric Key Cryptography

Asymmetric Key Cryptography

WHAT IF WE ADD ANOTHER KEY?

Two separate keys to secure data.

Whatever you lock with one key, can only be unlocked with the other.

It is not immediately apparent how this is an improvement but bear with me and I will show you what it means in terms of secure communications.

Keys Galore!

Everyone gets two keys!

- Public Key
- Private Key

Keys Galore!
Everyone gets two keys!
- Public Key
- Private Key

EVERYONE GETS TWO KEYS!
A PUBLIC KEY THAT YOU SHOUT OUT FROM ROOF TOPS. YOU WANT THE WORLD TO KNOW. (K+)
and a private key, you hold close to your heart and not even share with your dearest. (K-)
The wallet addresses of crypto currencies for example are public keys. You can't spend the money in the wallet without the private key.

PKE and Secure Communications

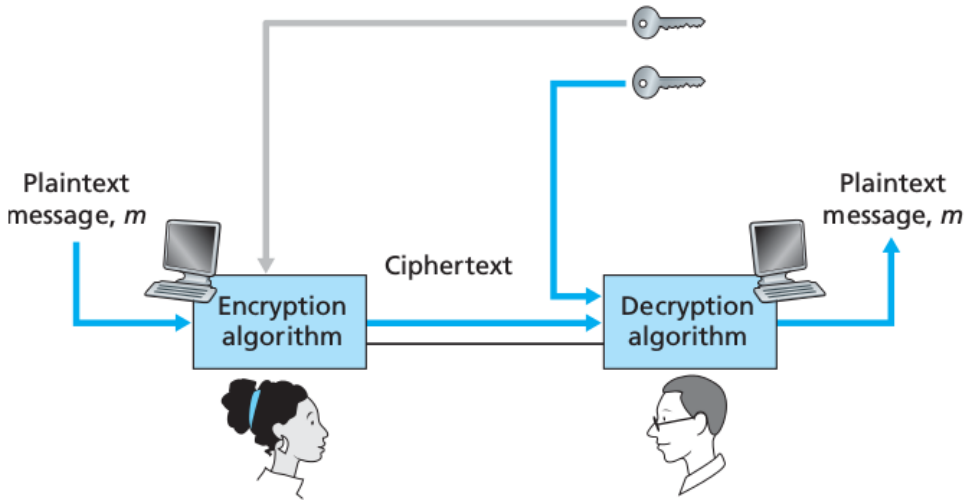
Let's remember:

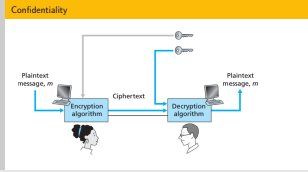
- Confidentiality
- Authentication
- Integrity

How can we achieve these with PKE?

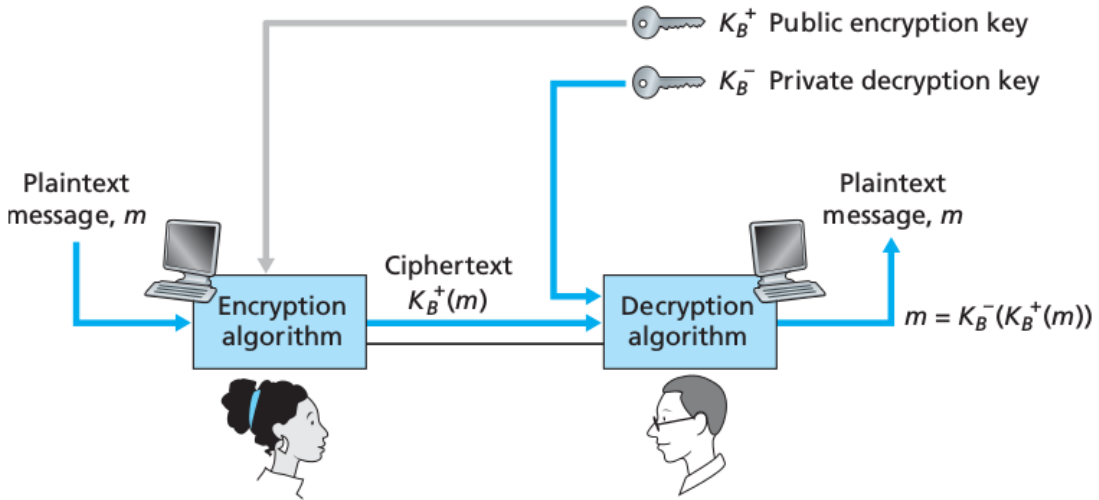
PKE and Secure Communications
Let's remember:
Confidentiality
Authentication
Integrity
How can we achieve these with PKE?

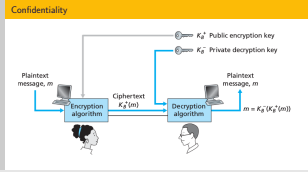
Confidentiality





Confidentiality

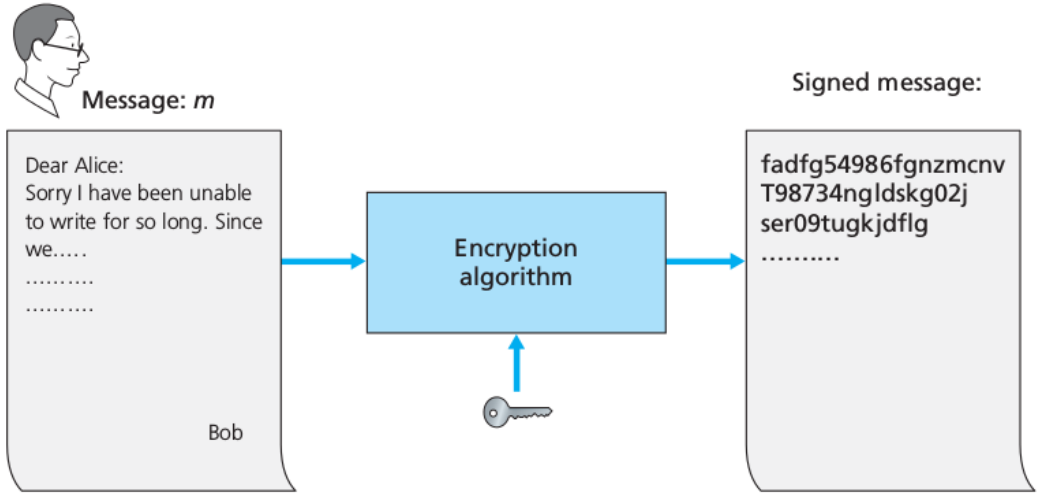


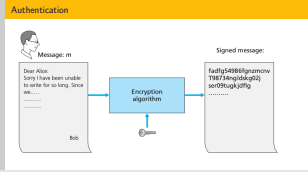


How can you ensure only the intended receiver can read your messages?

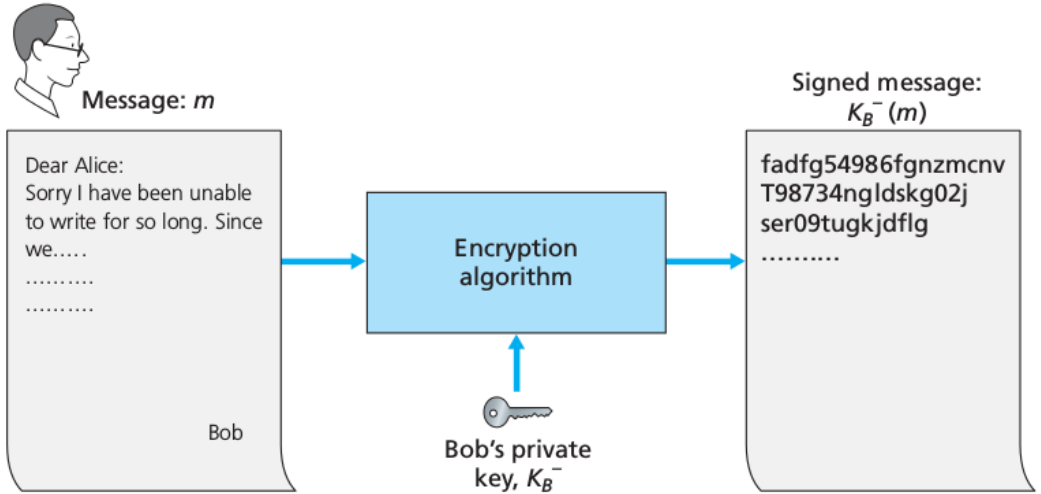
You have three keys in your hand. Your private/public key pair and your destination's public key pair. So you have three options.
You need to choose a key that threat actors (Trudy) along the way don't posses. So that your message gets accross unread.

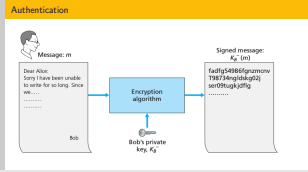
Authentication





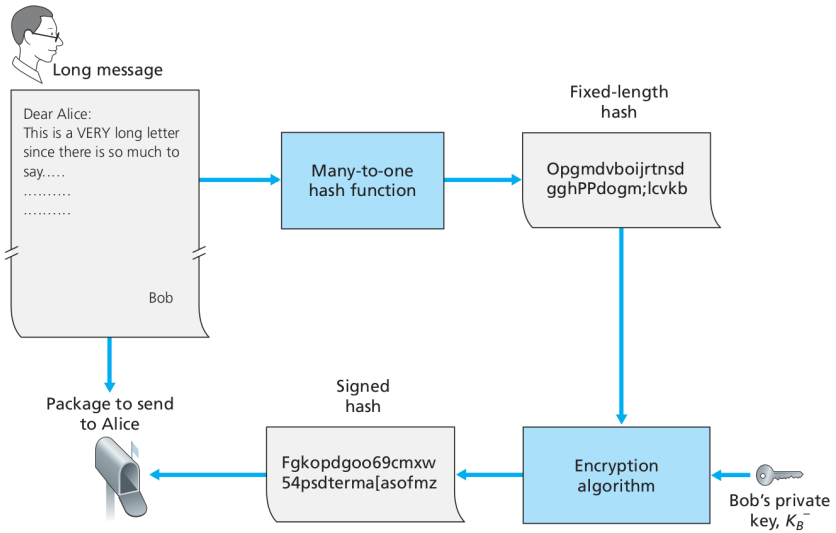
Authentication

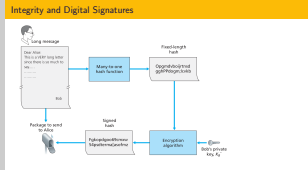




How can you make sure the receiving party knows for sure that you are indeed the sender?
Here you don't care if they can read the message or not. All you care about is if they can make sure it is you.
Again you have three keys in your hand, your own pair, and your destination's public key.
You need to pick a key that nobody else possesses, but everyone else can undo and prove that it was indeed locked by you.

Integrity and Digital Signatures





Before we get into it, here is something you need to know. A hash function is essentially a function that takes a long message and creates a short summary version of it. When you feed the same message, it always produces the same output.

Integrity: We want to make sure the message was unaltered.

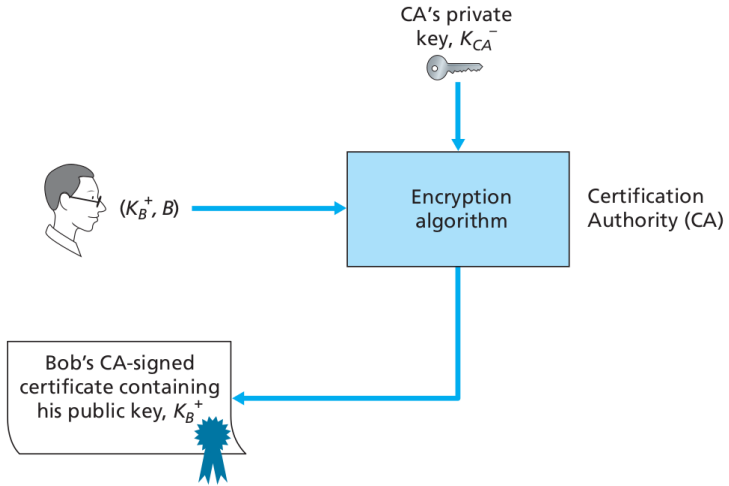
Sometimes you may need to broadcast a message. You don't care about confidentiality at all, infact you want everyone to be able to read the message. Like when you publish software on the internet. BUT! it is important to make sure the message is not changed and is indeed the same message you wrote. Like nobody inserted a virus into the software you published.

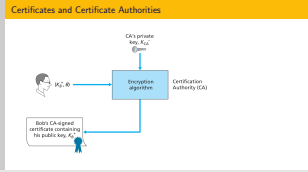
So you send the message, and encrypt a summary of the message with your private key (authenticating it is indeed you). That encrypted summary is called a digital signature.

Using your public key, anyone can make sure the hash they obtain from the message matches the one in your signature.

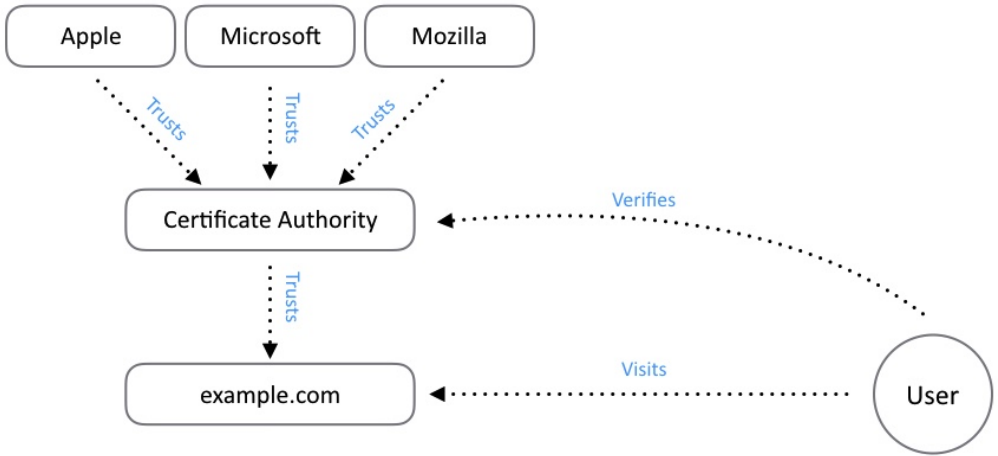
This is how we can make sure a message's contents are unaltered.

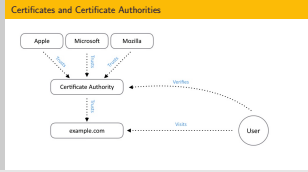
Certificates and Certificate Authorities





Certificates and Certificate Authorities





For it all to work, we need a reliable way to distribute public keys.
As anyone can create key pairs, we need to associate public keys with identities/entities.
That is where trusted third parties called Certificate Authorities come in.
CA's public keys are widely known. These are often bundled with operating systems and other relevant software.
When you register with a CA, they sign your public key. So anyone can verify that the public key was registered with a CA.
The signed public key (and a few details on identity) is called a certificate.
When you browse to your bank's website they send you one such certificate. So you can use CA's public key to decrypt the certificate and obtain the bank's public key.

Certificate Authorities, what could go wrong?

If there is a CA out there with wide spread acceptance.
They may abuse their position to facilitate man in the middle attacks.
Or if the CA does not practice due diligence, they may "accidentally" provide certificates for a domain already registered.
Multiple governments that have control of a Certificate Authority have issued certificates that can allow them to eaves drop on encrypted communications in the past (Kazakhstan, India, China...).

Asymmetric Key Cryptography and Data in Transit

Ideal for communication

Overhead is a problem

In combination with Symmetric key encryption.

Asymmetric Key Cryptography and Data in Transit
Ideal for communication
Overhead is a problem
In combination with Symmetric key encryption.

As we have seen, the nature of PKE makes it useful for securing communications.
Yet the computational overhead of PKE makes it slow for real time applications.
Hence in reality, PKE is only used to authorize and exchange shared keys.
Once two sides share keys through, PKE, they switch to symmetric key cryptography for the rest of the session.

Recap

- The Need for Multiple Keys
- Asymmetric Key Cryptography
- Confidentiality, Integrity, and Authentication (the other A)

Recap
- The Need for Multiple Keys
- Asymmetric Key Cryptography
- Confidentiality, Integrity, and Authentication (the other A)

Internet is a jungle. It can be beautiful but you need to watch out for yourself. Things you do online have consequences IRL.