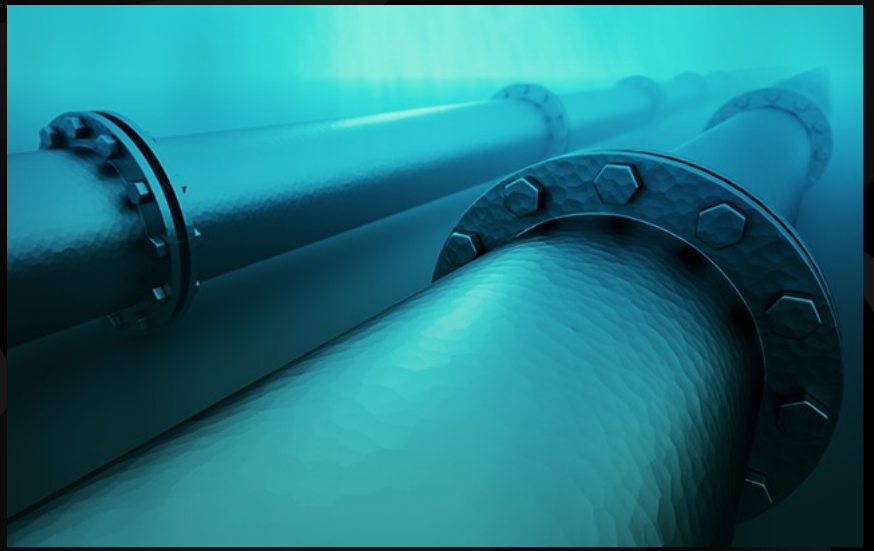
worteks
make IT work, make IT free

PARIS OPEN SOURCE SUMMIT

TLS for Dummies



Maxime Besson
info@worteks.com

Vorteks
make IT work, make IT free

(\vɔʁ.tɛks\)

PARIS OPEN SOURCE SUMMIT

Services

Heterogeneous and complex infrastructures, cloud, mail, authentication, security

- **Studies, audit and consulting**
- **Technical expertise**
- **Technical support**
- **Training**
- **R&D**

V'Sweet — **Collaboration and application portal**

V'Opla — **Mutualized platform for development**

FUSION IAM — **Identity and Access Management**

Partnership

BlueMind

redhat. READY BUSINESS PARTNER

In this talk

A tiny spoonful of cryptography

Public Key Infrastructures, Certificate Authorities

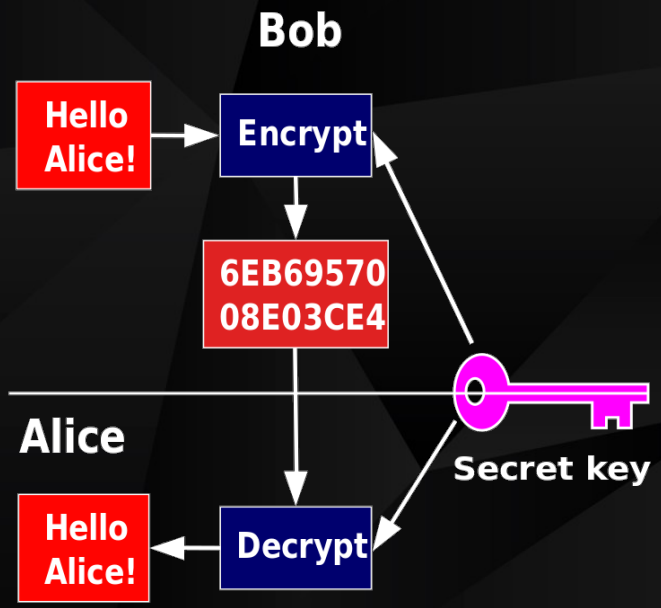
Different types of security

Our goal

We want to secure communication between two people

- On the internet

Symmetric-key cryptography

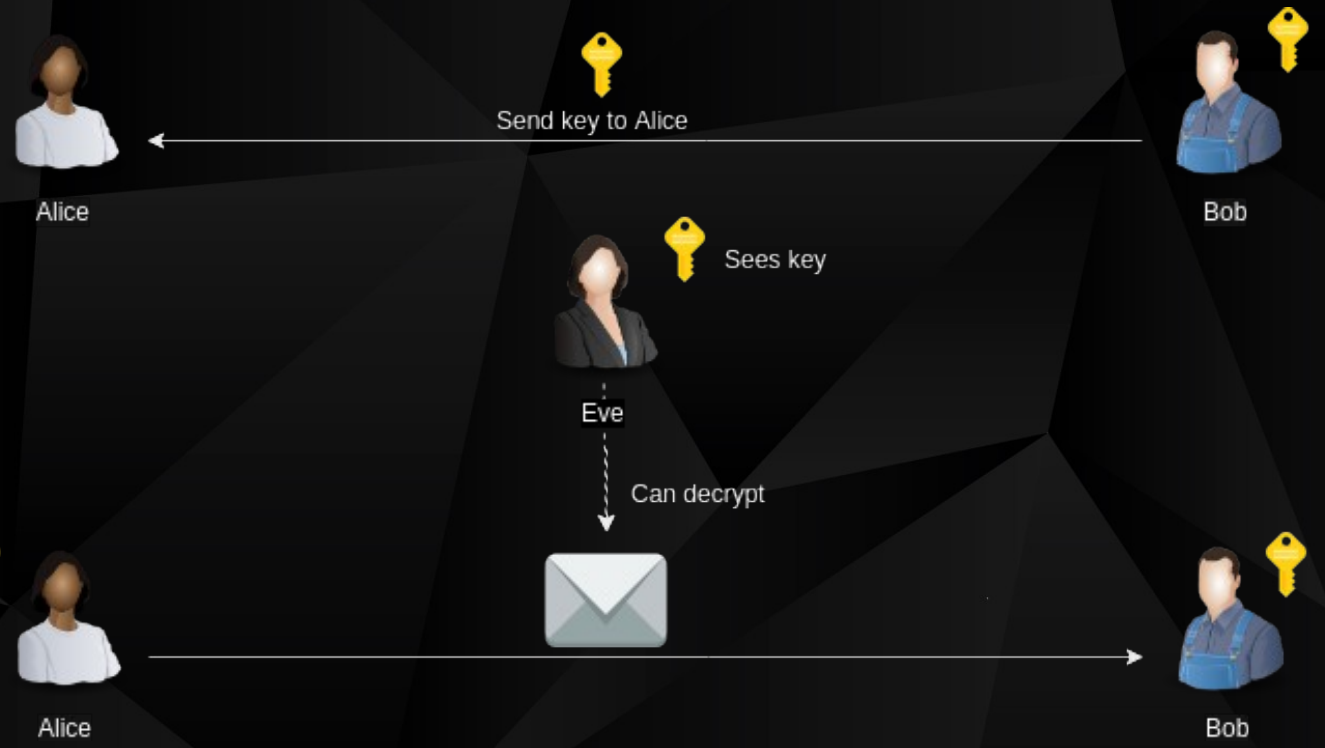


Looks good, let’s do that

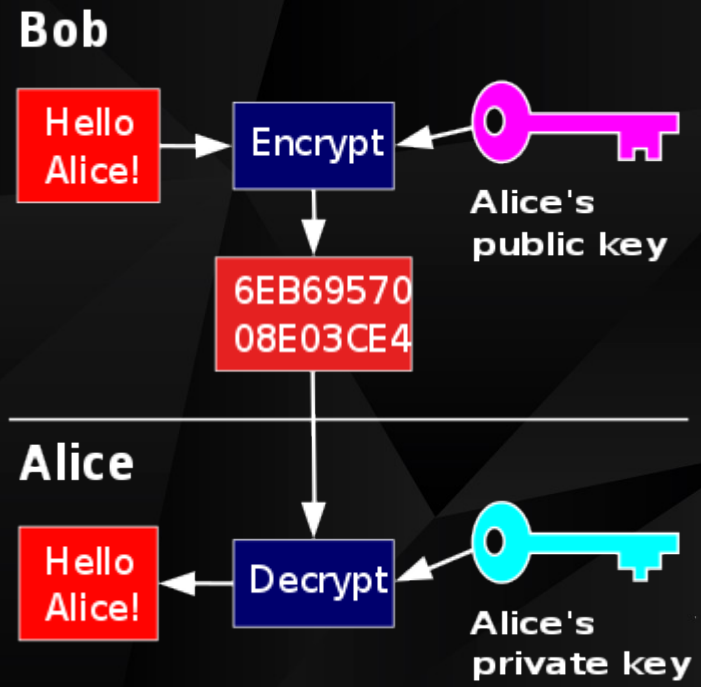
But wait, how do you exchange the key in the first place

Can’t do that on the internet, it’s full of eavesdroppers

Symmetric encryption



Public key encryption



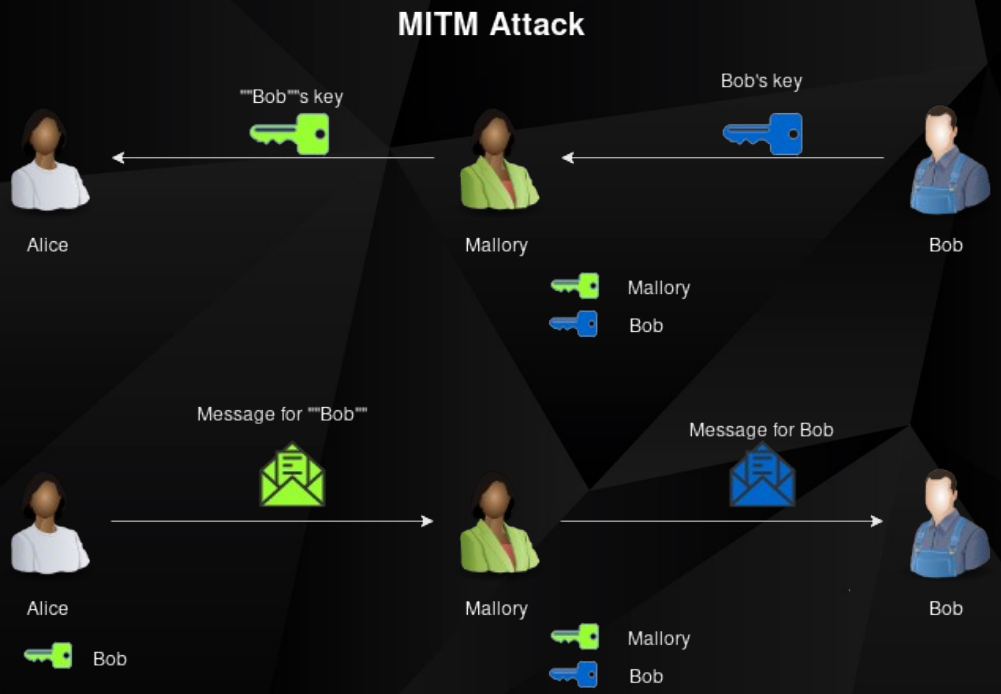
And how does this help us?

If Bob sends us his public key, we can send him a message that only he can decrypt

Eve is defeated!

But wait....

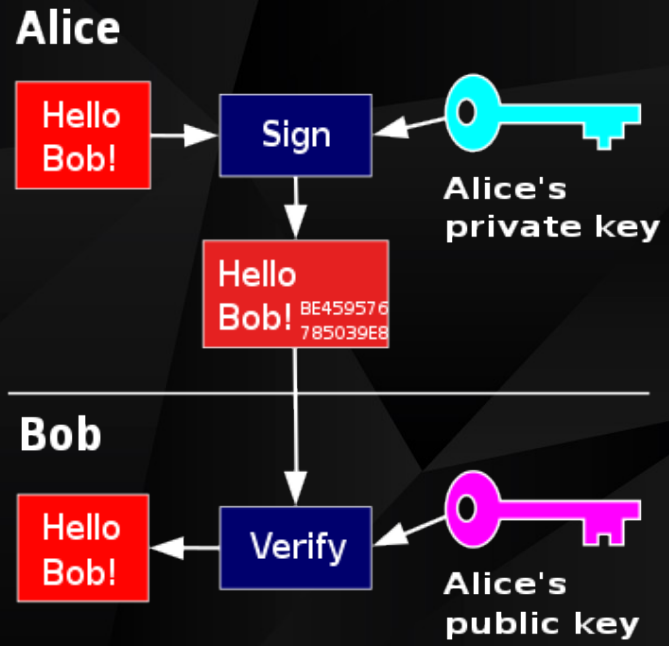
The (wo)man in the middle



Damned, foiled again

- How can we make sure that Bob’s public key belongs to Bob?

Signature


Alice
Hello Bob!
Sign
Alice's private key
Hello Bob! BE459576 785039E8
Bob
Hello Bob!
Verify
Alice's public key

So…

Our original goal was confidentiality

Signature is a different security property: it proves authenticity

Often combined with a hash function for integrity

How does signature help us

- Bob’s key cannot be signed by Bob because we don’t trust his key yet.
- We need a trusted third party

Trusted third party

Certificate Authorities

- Organizations that deliver certificates
  - A document containing a public key, and identity, and some metadata
  - A signature by the CA’s private key binds links them together
- The security of the whole is only as good as the security of the verification process
  - Mallory can try to have her public key cerfied as Bob’s!

Does it help us?

Yes, if everybody trusts the Certificate Authority, then all we need to have is the CA’s public key, and we can communicate with anybody!

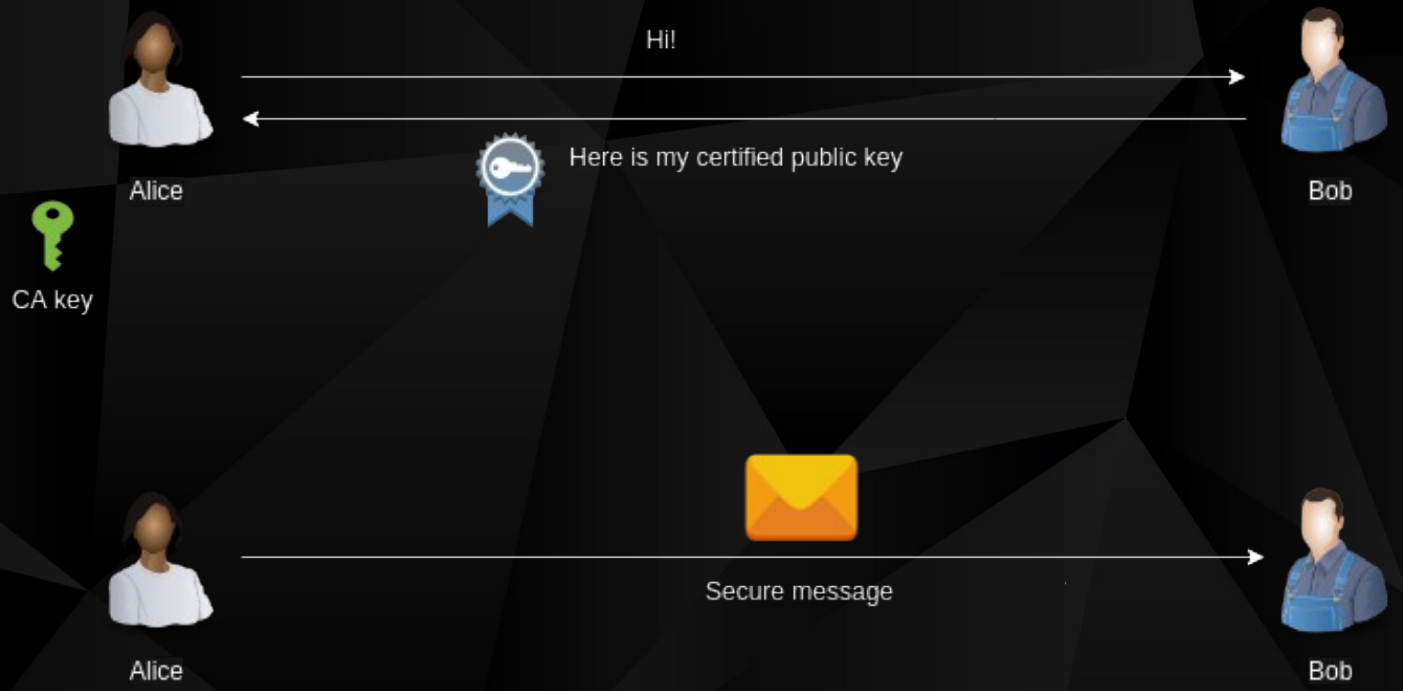
Public Key Infrastructure

A system based on Certificate Authorities is one but many possible ways to distribute public keys

Such systems are called Public Key Infrastructures

- There are other types (web of trust, blockchain...)

Let’s sum it up



Finally, a secure system

(If you don’t mind the all-powerful CA at the center of it all)

Every time either participant wants to send something, it needs to encrypt it with the other participant’s public key

What could go wrong ?

Too slow !

Public key cryptography is just too slow

But you know what isn’t?

- Symmetric cryptography
- But it’s insecure!

UNLESS!

Best of both worlds

Keys are just messages

We can generate a symmetric key

Send it securely using public-key cryptography

And then, immediately start using it

That way, the performance penalty is only used at the beginning of the connection

Our current scheme

Congratulations

- We just invented TLS!

TLS, in broad strokes

Phase 1: Authentication and key echange

- The server authenticates to the client
- Sometimes, the client also authenticates to the server
- Key exchange occur

Phase 2: Data exchange

- Uses symmetric encryption

Imagine the following scenario

Alice

Hi Bob!

Evil hacker posing as Bob

Hi Alice, here is my certified public key

CA key

Public key certified to belong to Wile. E. Hacker

Certificate validation

When receiving a certificate, we must make sure that

- It belongs to the person we wanted to talk to
  - For websites, it means that it was issued to the correct domain
- It’s not too old or too young
- It was signed by a trusted authority
- The signature is valid

TLS software does this by default

- Don’t disable it
- It will make Mallory very happy if you do

Certificate validation

A certificate ties a public key to an identity

The CA has to do its own verification

- Usually, you only need to prove ownership of the domain mentionned in the certificate
  - Anyone can get a certificate for https://this.is.google.i.swe.ar/
- EV certificates cover the legal entity behind the request
  - They are displayed as a green bar with a company name

Reality is complicated

- In reality, we don’t JUST use a symmetric cipher
  - Integrity is guaranteed through HMAC or AEAD
- There are many versions of TLS
  - SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3
    - Use TLS 1.2, and start planning for TLS 1.3
- Diffie-Hellman key exchange ensures perfect forward secrecy
- There are many algorithms and parameters
  - Usually auto negotiated, but...

worteks
make IT work, make IT free

PARIS OPEN SOURCE SUMMIT

Thanks for your attention

More informations:


info@worteks.com


@worteks_com


linkedin.com/company/worteks

Channel security

- CAs like being ambiguous about this
- The strength of the symmetric cipher has NOTHING to do with certificates
  - Except obsolete SGC
- But if the certificate is too weak, you are at risk of MITM
  - You can have a super-strong secure channel to a hacker’s computer

Will TLS make my website slower

Short answer: no

Long answer:

- It makes connection slower
  - It’s worth it
  - Use keepalive
- If you are using modern CPUs, the overhead of the symmetric cipher is insignificant

What the hell are Elliptic Curves

A mathematical tool used in cryptography (ECC)

Used in public key encryption, so only during the certificate phase

They use smaller keys than the previous RSA scheme

- Faster connection time
- Lower CPU consumption