Criptografía e infraestructura de clave pública

Principios de la seguridad informática

¡Importante!!

Confidencialidad

solo personas autorizadas

Integridad

Ni alterada ni modificada

Disponibilidad

Recursos disponibles y accesibles

Autenticidad

Veracidad de auditoria

Criptografía

Se encarga del estudio de los **algoritmos, protocolos y sistemas** que se utilizan para dotar de seguridad a las comunicaciones, a la información y a las entidades que se comunican

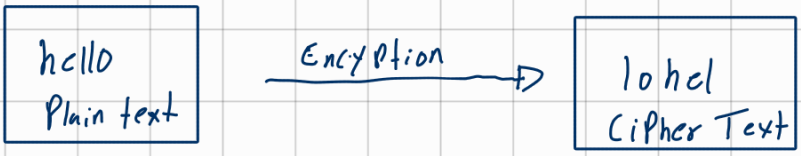
Esta mamada dice que necesitamos asegurar la seguridad de la mierda que mandemos a traves de internet, porque no sabemos que mierda pase ahi

Para ello hay 2 formas, el cifrado Punto a Punto, y Transporte

Encryption

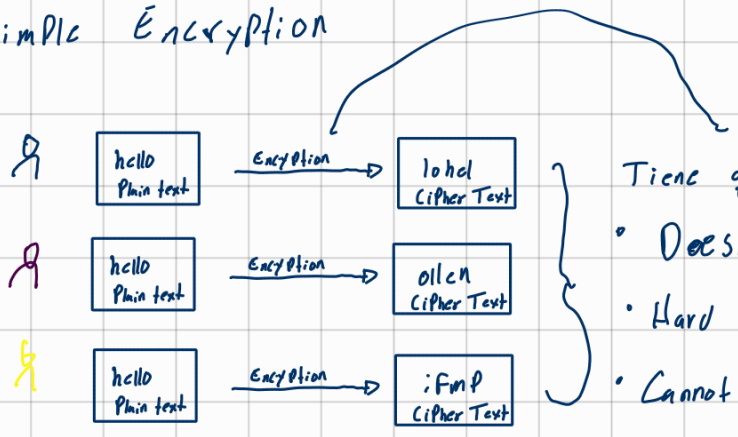
Encryption is used to Provide Confidentiality

↳ Confidentiality : Only intended recipent can interpret the data



- Plain Text : Data before encryption
- Cipher Text : Data while encrypted

- Simple Encryption



Tiene que estar haciendolo diferente

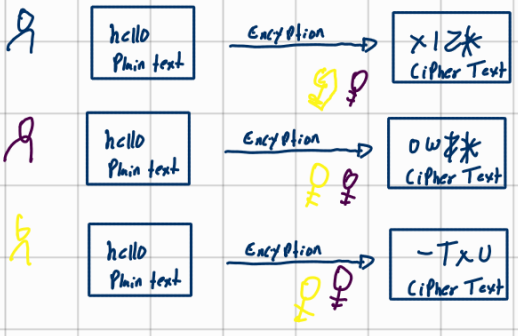
- Doesn't Scale
- Hard to do securely
- Cannot simply use a Standard Algorithm

- Key Based Encryption

↳ Combines industry vetted algorithm with a secret key

↳ algorithm is created by experts

↳ Secret keys can be randomly generated



Encryption

Two types of Key Based Encryption:

- Symmetric Encription → Encrypt and Decrypt using the same Keys
- Asymetric Encription → Encrypt and Decrypt using different Keys

Encryption

abcdefghijklmnopqrstuvwxyz

- Asymmetric Encryption:

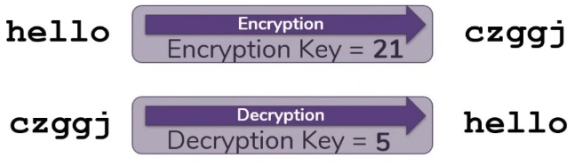
Two different keys that are mathematically related

- Symmetric Encryption:

Encryption

abcdefghijklmnopqrstuvwxyz

- Asymmetric Encryption:



- Two different keys that are mathematically related
- What one key Encrypts, only the other can Decrypt
  - One key will be made Public →
  - Other key will be kept Private →

We will discuss Public and Private Keys in more detail in a later lesson

Encryption

- Asymmetric Encryption — Restricted to Limited Data
  - Weakness: Slower – Requires much larger key sizes
  - Weakness: Cipher text expansion
  - Strength: Private Key is never shared – More Secure
- Symmetric Encryption — Ideal for Bulk Data
  - Strength: Faster – Lower CPU Cost
  - Strength: Cipher text is same size as Plain Text
  - Weakness: Secret key must be shared – Less Secure

https://youtu.be/o_g-M7UBqI8?si=0YywDnvFl1o4deik

Encryption

- Asymmetric Encryption algorithms: — Restricted to Limited Data
  - DSA
  - RSA – Recommended Key Size: 2048 bits
  - Diffie-Hellman
  - ECDSA
  - ECDH
- Symmetric Encryption algorithms: — Ideal for Bulk Data
  - DES 56 bit key
  - RC4 128 bit key
  - 3DES 168 bit key
  - AES 128, 192, or 256 bit keys
  - ChaCha20 128 or 256 bit keys

Cifrado simetrico → Utiliza la misma clave para cifrar y descifrar

Cifrado asimetrico → Utilizan claves distintas o Pueden utilizar claves distintas Para cifrar

Pinche repaso de youtube we, tarde o temprano ya tenia que llegar aqui

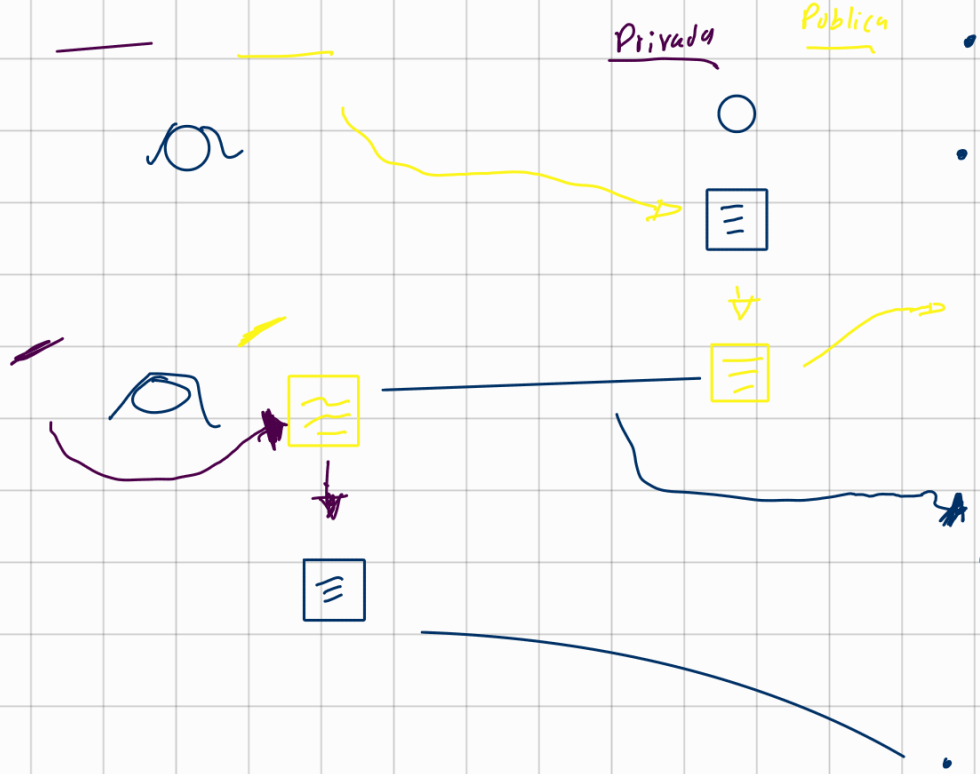
Public and Private Keys

Asymmetric Key Pair can be used for: Encryption → & signatures

We're going to use Pam and Jim they're going to use asymmetric keys to securely exchange data with one another, now since these two are two different People, they each have their own set of Public an Private Keys

Pam has one set of Public an Private Keys, she has her Public Keys closer to Jym available to Jym, if he needs it and she has their Private Key hidden Private from anybody else

Jim also has his own set of Public and Private Keys and like we discussed in the las lesson, what is encrypted with this Public Key can only be decrypted with this Private Key and vice versa



- Jim wants to send a secret message to Pam
- Jim use Pam's public Key to encrypt the message

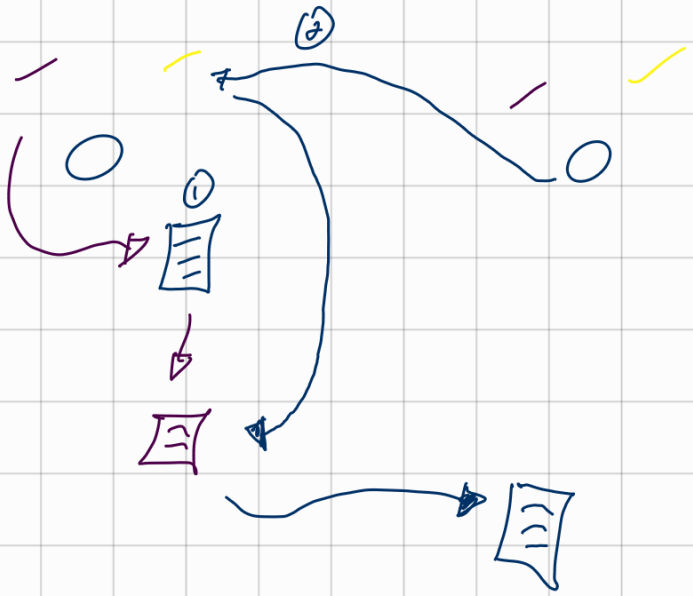
Ahora, la unica llave que puede desencriptarlo es la llave privada de PAM

Este mensaje puede ser enviado a traves de la red Con seguridad

- Only the correlating Priva. te Key can decrypt

And this is how asymmetric Keys are used to Provide confidentiality, recall that confidentiality is the idea that the data is only accessible to the intended recipient

Otro ejemplo



1) A PAM le vale verga que lo vean pero quiere Probar que ese mensaje es se ella.

2) Asi que usa su llave Privada, Para que la unica llave que Pueda descriptarla sea su llave Publica

Integrity

Jim Know message was not modified in transit

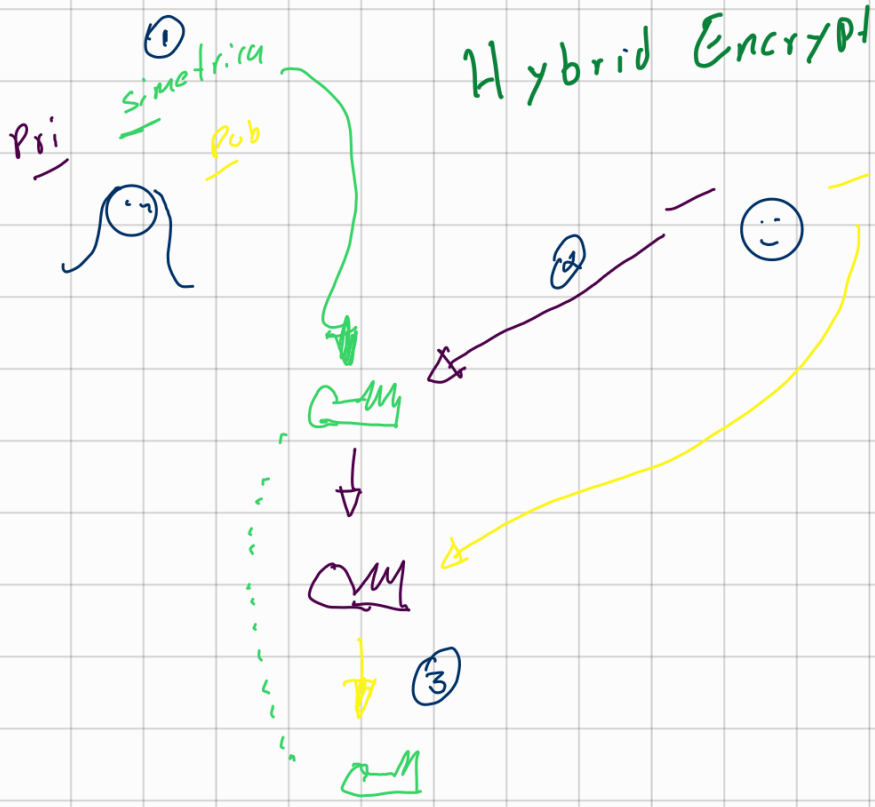
Jim knows Pam Most have sent the message == Authentication

if Jim can decrypt the message, this actually Proves two things:

Public and Private Keys

- Asymetric Key Pairs can Provide Encryption and Signatures
  - But... in reality it is not than simple
  - Remember, Asymetric encryption has limitation
    - Can't use for bulk data, but can use it for limited data
- Bulk data should be protected with Symmetric Encryption

What if we used Asymmetric Keys to share Symetric Keys that is what SSl and TLS actually do



(1) Pam randomly generates a symetric secret K

(2) Pam encrypts Symmetric Key with Jim's Public Key

(3) Jym decrypts Symmetrics Key with Jim's Private Key

- Bulk data can now be Symmetrically encrypted

Porque ya los 2 tienen la misma llave

Hybrid Encryption → Concept of using both Asymmetric and Asymmetric Encryption

- Asymetric encryption to facilitate a Key Exchange
- Secret Key used with Symetric Encryption for Bulk data

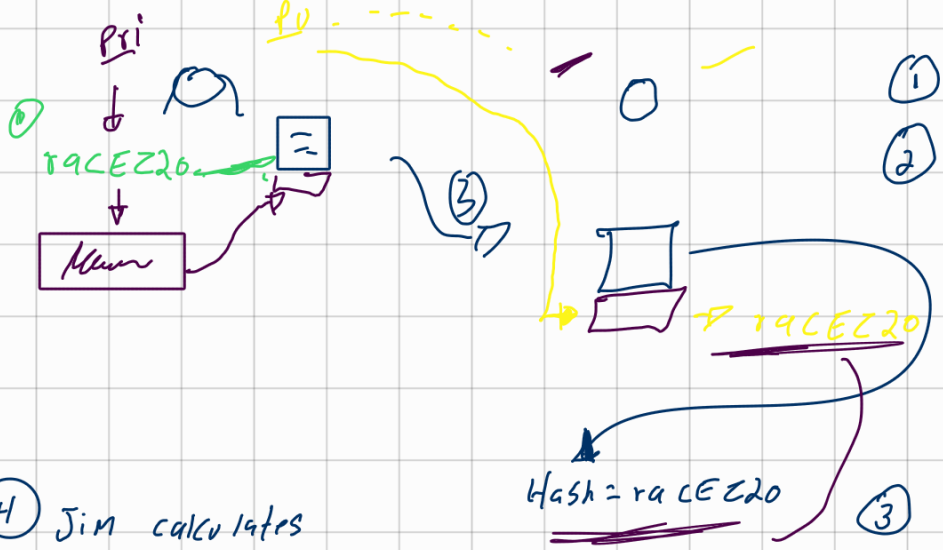
But what about Signatures?

- Entire message can't be "encrypted" with Pryvate Key
  ↳ Again, Asymetric encription has limitations
- Could we sign a fixed, representational sample of the message?
  - Hashing algorithm

↳ Algorithm which takes as input a message of arbitrary length and Produces as output a "finger Print" of the Original message

hello ⟶ 8+5+12+12+15 ⟶ 52

Process for using an Asymetric Key pair for Signatures:



① PAM calculates the hash

② PAM encrypts resulting digest with Pam's Private Key

- This is the actual Signature
- Signature is appended to the message

③ Jim decrypts the Signature

Son iguales? with Pams Public Key

si → todo bien NO → alterado

④ Jim calculates

Hash of received message

Process for using an Asymmetric Key Pair for Signatures:

- if both digests match, this proves two things:
  - message hasn't changed since Pam signed it → Integrity
  - Only Pam could have created the signature → Authentication