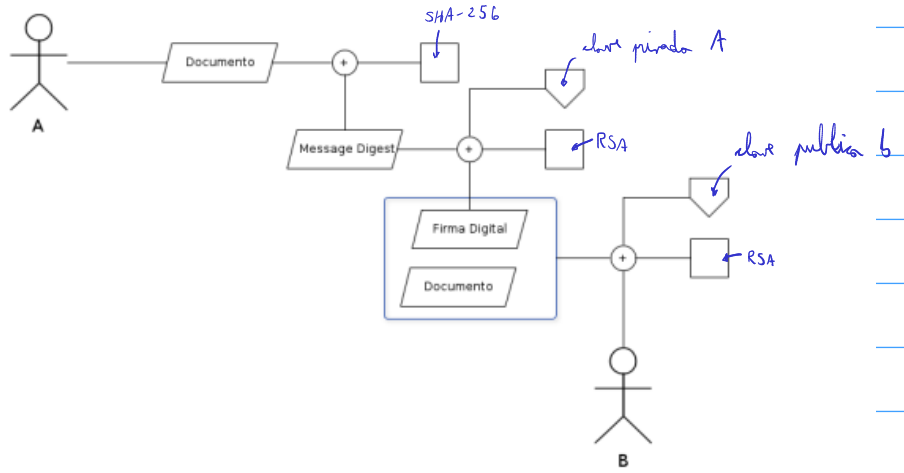
A desea enviarle un mensaje a B de carácter importante. A quiere asegurarse de que nadie excepto B pueda leerlo y que B pueda confiar en que A fue quién envió el mensaje.

a. Basandose en el esquema a continuación, completando los cuadrados con algoritmos y las casitas con los parámetros adicionales que estos toman, explique cómo puede hacer A para construir el mensaje usando criptografía asimétrica, de manera de garantizar las propiedades de Confidencialidad y No repudio.

b. Explique qué debe hacer B para verificar que A fue quién envió el mensaje.

- **Confidencialidad.**
- **Integridad.**
- **Autenticación.**
- **No Repudio.**
- *Disponibilidad.*



Yo tengo mi bello documento y lo hasheo SHA-256 2:06 a. m.

Ahi tengo el msg digest, eso lo encripto con mi privada y ahi como que lo firmo porque solo yo le puedo poner mi privada RSA 2:06 a. m.

De ahi consigo la bella "firma digital" 2:07 a. m.

Despues agarro esa firma, agarro el documento original y los encripto con tu clave publica RSA 2:07 a. m.

Y ese paquete es el que te llega a vos 2:07 a. m.

Entonces vos mandas tu clave privada y obtenes el documento mas la firma
Confidencialidad porque solo brunito tiene su clave privada 2:08 a. m.

A priori si te da paja ver quien soy ya podes ver el documento igual 2:08 a. m.

Pero si estas en modo detective le podes pasar la publica a mi firma
No repudio porque si el msg digest da bien solo yo la puedo haber encriptado 2:08 a. m.

Y ahi obtenes el msg digest 2:08 a. m.

Y ahi haces el famoso if 2:08 a. m.

Brunito decime que logré ver la matrix 2:08 a. m.

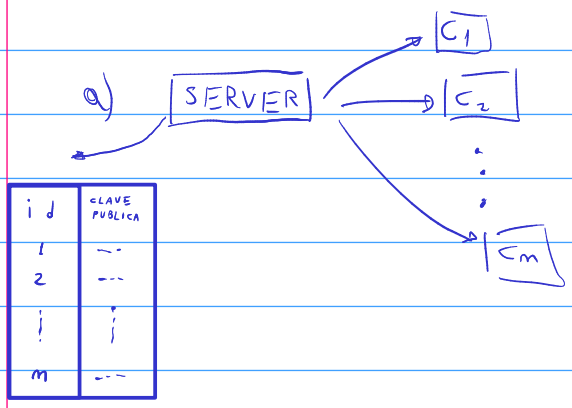
Suponga que una compañía necesita implementar un sistema que garantice la autenticidad de sus clientes usando un sólo servicio instalado en un servidor.

a. Se sabe que ssh admite autenticación por clave pública y privada mediante el método de challenge-response. Explique dónde y cuántas claves públicas y privadas deberían instalarse para que se pueda garantizar la autenticidad de los clientes usando ssh.

b. Suponga ahora que los clientes necesitan garantizar la autenticidad del servidor de la compañía, ¿Dónde deberían instalarse las claves públicas y privadas?

c. También se puede garantizar autenticidad estableciendo una conexión SSL/TLS que usa un handshake seguro intercambiando certificados digitales. Explique cómo cambian la soluciones de los incisos a. y b. si la compañía dispone de un certificado digital propio firmado por una autoridad certificante.

a)



Cae el server y te dice "La contraseña es HSMTMTS", pero no te lo dice en español como un buen hijo de vecino. Lo encripta con tu clave publica y te manda el msg al grito de "Contestame si la clave te queda gil".

Vos que sos un habil contestador te sacas la clave privada que tenes siempre guardada en el bolsillo de tu calzon, desencriptas el msg y le decis: "A mi me parece que el gil aca sos vos, HSMTMTS 👆🏽"

El server, con la dignidad por el piso no tiene otra opcion que bajar la cabeza y someterse al cliente.

b) Es basicamente lo mismo, pero ahora el server tambien tiene un par de claves y todos los clientes tienen la clave publica del server.

Ahora no solo es el server quien apura a los clientes, si no que los clientes, con el afan de no ser cagados, ademas de contestarle la contraseña al server le presentan su propio desafio encriptado con la clave publica del server.

El server, nervioso porque generalmente es el quien se encuentra en la posicion de poder, busca con sus manos temblorosas su clave privada, luego de encontrarla en el bolsillo de su sombrero pescador resuelve el desafio, no sin antes devolverle al cliente el bello gesto recibido en el challenge 👆🏽.

c) Ahora pusiero platita y todo este tema de autenticacion se va a hacer con TLS/SSL.

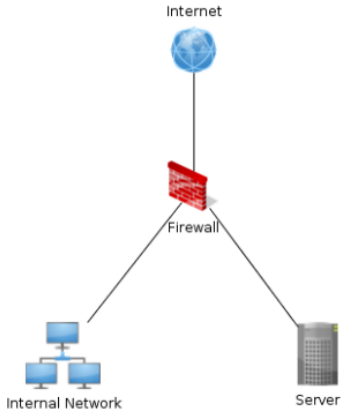
Primero que nada, todas las máquinas tienen que tener instalado un certificado de una autoridad certificante (CA) que contiene su clave pública: K^+_{CA}. Luego, para garantizar la Autenticidad de los clientes C_i, cada uno de estos debe generar un par de claves pública y privada $(K^+_{C_i}, K^-_{C_i})$, construir un certificado con la clave pública $(K^+_{C_i})$ y hacerlo firmar por la autoridad certificante de manera que lo asocie con el nombre del cliente (C_i). El certificado que se debe instalar en cada cliente contendría las siguientes piezas de información:

$$(\, C_i;\, K^+_{C_i};\, F_{CA,C_i}),\ \text{con}\ F_{CA,C_i} = E(H(C_i + K^+_{C_i}), K^-_{CA})\,)$$

Donde E es un algoritmo de encripción de clave asimétrica y H es una función de Hash. Luego, se instala cada certificado en cada cliente para que se envíe durante el Handshake SSL y que el servidor pueda garantizar la autenticidad usando K^+_{CA} para validar el certificado y, luego, $K^+_{C_i}$ para autenticar al cliente. Finalmente, para garantizar la autenticidad del servidor, éste debe generar un par de claves pública y privada (K^+_S, K^-_S), generar su certificado, hacerlo firmar por CA e instalarlo en el servidor para su posterior envío en el Handshake SSL.

CHEQUEAR

El siguiente es un diagrama de una topología de la red interna de la compañía **Siliconsec**:



Donde los servicios provistos por **Server** son:

- Webserver con el sitio de la compañia
- HTTP Proxy
- DNS, Resolver y Autoritativo de Dominio
- Correo Saliente y Entrante

Configure el Firewall de tal manera que todos los servicios se encuentren disponibles para internet pero que los usuarios pertenecientes a la red local puedan:

- Acceder a internet vía proxy
- Leer y enviar correos