Teoría de las comunicaciones

Práctica 6: Seguridad

Temas:

Criptografía simétrica y asimétrica, Firma Digital, Certificados, Conexiones Seguras

Definiciones:

Mensaje: M

Criptograma: C

Digesto: D

Clave simétrica: K

Clave pública de A: K_A^+

Clave privada de A: K_A^-

Encriptar M utilizando la clave Q: $E_Q(M) = C$ con $Q \in \{K, K_A^+, K_A^-\}$

Desencriptar el C utilizando la clave Q: $D_Q(C) = M$ con $Q \in \{K, K_A^+, K_A^-\}$

Aplicar Función de Hash Criptográfico: $H(M) = D$

Aclaración: La notación permite combinar cada algoritmo con cada tipo de clave para obtener distintos resultados. No todo algoritmo permite toda clave. Deberá aclararse qué algoritmo es el utilizado.

Ejercicio 1

Del siguiente criptograma se conoce que las letras fueron encriptadas usando un cifrado *César*.

```
pm fvb aopur aljouvsvnf jhu zvscl fvby zljbypaf
wyvisltz, aolu fvb kvua buklyzahuk aol wyvisltz
huk fvb kvua buklyzahuk aol aljouvsvnf.
--iybjl zjoulply
```

Describa una estrategia que se pueda usar para descubrir el desplazamiento.

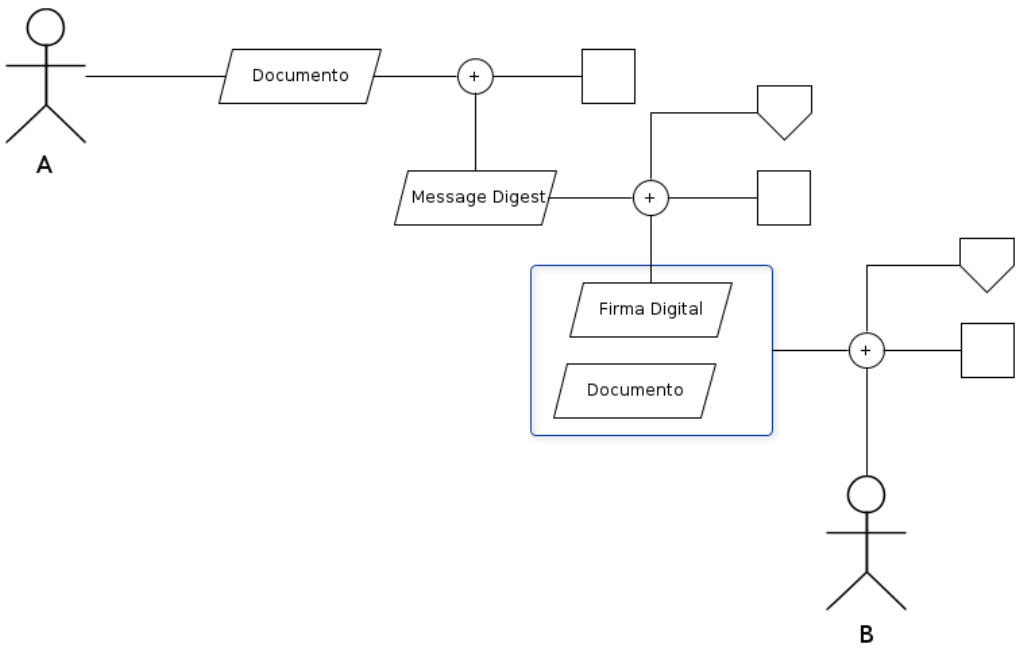
Asumir: que el texto original contenía letras sin tildes

Ejercicio 2

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.



Ejercicio 3

A y B utilizan criptografía asimétrica para garantizar la confidencialidad sobre los mensajes que se envían. Para que puedan asegurarse que sus mensajes no sean leídos por nadie más, primero deben intercambiar sus claves públicas.

a. Explique cómo se puede vulnerar la confidencialidad de la comunicación entre A y B si alguien intercepta el intercambio de claves públicas.

b. Explique qué piezas de información tienen los certificados digitales y cómo se usan para solucionar éste problema.

Ejercicio 4

Muchos protocolos para establecer conexiones seguras usan handshakes para iniciar el sistema criptográfico. En este ejercicio tenga en mente SSL/TLS como sistema criptográfico a analizar.

a. De los siguientes parámetros indique la etapa del algoritmo donde se utiliza: $HELLO$, $Key - Exchange$ o $Data - sharing$.

- Parámetros Criptográficos
- Valor al azar
- Conjunto de Algoritmos de encripción
- Versión Protocolo
- Certificado del destinatario (Peer)
- Clave Maestra (Masterkey)
- Criptograma

b. Muestre mediante un diagrama de secuencia una posible implementación de un handshake para establecer una conexión. Considere los mensajes enviados, y si se envían en plano o como criptogramas.

Ejercicio 5

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.

Ejercicios de Parcial

Ejercicio 6

Una organización nos pide que implementemos una política de seguridad para su red. Dicha compañia desea que sólo usuarios autenticados puedan acceder a recursos Web en Internet conectandose mediante HTTPS con el Proxy. Explique cómo hacer para garantizar la autenticidad de los usuarios del lado del Proxy, aclarando dónde se instalarían los certificados digitales.

Ejercicio 7

En el hall de un hotel hay un WiFi donde los huéspedes pueden conectarse y navegar en internet usando sus dispositivos móviles. Se desea que sólo puedan navegar la Web via un servidor *Proxy*. Repetidas veces, hackers han espiado las peticiones de los clientes. Diseñe un sistema criptográfico de clave asimétrica, que garantice la autenticidad del proxy y la confidencialidad de los clientes. Aclare dónde deberían instalarse los certificados.

Ejercicio 8

Es recurrente en la empresa que ocurran peleas internas entre los empleados endilgandose la responsabilidad por tareas no realizadas. Por lo tanto se solicita implementar algún mecanismo para garantizar la propiedad de NO REPUDIO en todos los mensajes que se mandan internamente. Describa un mecanismo posible para lograr el requerimiento.

Ejercicio 9

La empresa Security First expone una API usando el protocolo HTTP. Dicha API tiene un método *getPrice* que devuelve el precio de frutas usando la siguiente url: `http://api.securityfirst.com/?method=getPrice&fruit=Pera`.

a. Es necesario agregar un método nuevo a la API que haga lo mismo que el getPrice pero que provea el servicio sólo a usuarios autenticados brindando **integridad** y **no repudio** del lado del servidor sobre los pedidos de los usuarios.

   1. Explique qué información tiene que tener el cliente y el servidor para que esto sea posible.
   2. Muestre una posible url que permita procesar el pedido.
   3. Explique qué es lo que tiene que hacer cada parte para garantizar lo solicitado.

   Nota: Es requisito para lo anterior no usar encripción sobre la totalidad del mensaje y no manejar sesiones.

Bibliografía

Computer Networks: A systems approach. 5ta Edición. *Peterson & Davie.* Capítulo 8: Network Security.