Capítulo 1 - Introducción

1. Criptografía y criptografía moderna.

Historicamente: ámbito militar y organizaciones de inteligencia.
Hoy: en todos los ámbitos. Por ej: información digital segura, transacciones y cálculos distribuidos.

2. El marco de la encripción de clave privada

Antes: cifrados (**ciphers**). Ahora: esquemas de encripción (**encryption schemes**)

Private Key Setting:

- Dos participantes comparten una información secreta: la clave.
- El participante que envía el mensaje usa la clave para encriptar.
- El receptor usa la misma clave para desencriptar y recuperar el mensaje original.
- El mensaje se lo denomina texto plano.
- La información transmitida es el texto cifrado.
- Clave simétrica: porque es la misma para encriptar que para desencriptar.
- Requiere que las partes compartan una clave de manera secreta.

Sintaxis de encripción

Un esquema de encripción de clave privada comprende tres algoritmos.

1) **Gen :** Algoritmo probabilística que emite una **clave k**. Se elige de acuerdo a alguna distribución determinada por el esquema. **k←Gen()**
2) **Enc :** Algoritmo que toma como entradas la **clave k** y **texto plano m** y emite como salida un **texto cifrado c.** **$Enc_k(m)$**
3) **Dec:** Algoritmo que toma como entrada la **clave k** y **texto cifrado c** y emite como salida un **texto plano m**. **$Dec_k(c)$**

Espacio de claves K **:** es el conjunto de todas las posibles claves que puede obtenerse a través de Gen.
Espacio de mensajes M : es el conjunto de todos los posibles mensajes.
Espacio de cifrados C .

Un esquema de encripción queda completamente definido al especificar los tres algoritmos y el espacio de mensajes

Además, debe cumplirse que **$Dec_k(Enc_k(m)) = m$**

Principio de Auguste Kerckhoffs:
No se requiere que el método de cifrado sea secreto, y hasta puede caer en manos del enemigo sin inconveniente.
La seguridad debe recaer únicamente en que **la clave se mantenga en secreto**.

Argumentos a favor de este principio:

1. Es más fácil mantener en secreto una clave que mantener en secreto un algoritmo.
2. En caso de que la clave sea descubierta, es más fácil cambiar la clave que cambiar el algoritmo.
3. Si muchas personas deben encriptar cosas, es más fácil que todas usen el mismo algoritmo y diferentes claves, y no al revés.

Escenarios de ataques:

- **Ataque de texto cifrado.** (**ciphertext only attack**) PASIVO

El adversario sólo observa el texto cifrado.
Intenta determinar el texto plano.

- **Ataque de texto plano conocido** (**known-plaintext attack**) PASIVO

El adversario obtiene pares (plano, cifrado)
Intenta determinar el texto plano correspondiente a otro texto cifrado.

- **Ataque de texto plano elegido (chosen-plaintext attack)** ACTIVO

El adversario tiene la posibilidad de obtener la encripción de textos planos de su elección.
Intenta determinar el texto plano correspondiente a otro texto cifrado.

- **Ataque de texto cifrado elegido (chosen ciphertext attack**) ACTIVO

El adversario tiene la posibilidad de obtener la desencripción de textos cifrados de su elección.
Intenta determinar el texto plano correspondiente a otro texto cifrado, cuya desencripción NO puede obtener en forma directa.

3. Cifrados históricos y su criptoanálisis

Cifrado César
Cifrado de rotación.
Es posible efectuar un ataque por fuerza bruta (búsqueda exhaustiva)

Principio del espacio de claves:
Un esquema de encripción seguro debe tener un espacio de claves que no sea vulnerable a búsqueda exhaustiva. (Condición necesaria, pero **no suficiente**)

Ataque mejorado:

Tener en cuenta que: $\sum_{i=0}^{25} p_i^2 \approx 0.065$

Si la clave es k, se espera que q_{i+k} debería ser prácticamente igual a p_i para todo i.

Si calculamos $I_j = \sum_{i=0}^{25} p_i \cdot q_{i+j}$ para cada valor de j entre 0 y 25, se espera que encontremos que $I_k \approx 0.065$, donde k es la clave utilizada. (Se calcula I_j para todo j y se decide que si I_j es casi 0.065 entonces j = k)

Sustitución monoalfabética.
Hace corresponder a cada carácter de texto plano un carácter de manera arbitraria (según una relación biyectiva= permutación del alfabeto ➔ espacio de claves de tamaño 26!)
Un ataque de fuerza bruta no es posible, pero sí análisis de frecuencias.

Vigenere.
Aplica múltiples cifrados de rotación en secuencia.

Ataques:

Si se conoce la longitud de la clave, (período) es fácil.

Si no se conoce, ,se aplica el método de Kasiski: La distancia entre dos apariciones múltiples (de digramas o trigramas) es un múltiplo de la longitud del período. Etonces, primero se calcula el MCD entre todas las distancias entre secuencias repetidas y eso permite obtener el período.

Otra manera es con el índice de coincidencia.

Longitud de cifrado y criptoanálisis: En Vigenere, se necesitan largos fragmentos de texto cifrado para efectuar el criptoanálisis.

Ataques de texto cifrado solamente y ataques de texto plano conocido:
Los ataques descriptos son todos de texto cifrado solamente.
Un ataque de texto plano conocido es trivial en estos cifrados clásicos.

Lecciones importantes:

1. Un esquema de encripción seguro debe tener un espacio de claves que no pueda explorarse en forma exhaustiva. Sin embargo, no es suficiente.
2. El diseño de un cifrado seguro es una tarea ardua.

4. Los principios básicos de la Criptografía Moderna.

4.1. Principio 1: Formulación de definiciones exactas.

El primer paso para resolver un problema de criptografía es la formulación de una definición precisa y rigurosa de la **seguridad**.

1. Importancia para el diseño: si no se entiende bien qué se desea conseguir ¿cómo se puede saber si se ha conseguido?
2. Importancia para el uso: ¿cómo sabremos qué esquema de encripción usar? ¿cuál es mejor para nuestra aplicación?
3. Importancia para el estudio: Dados dos esquemas de encripción, ¿cómo se pueden comparar?

Definiciones de seguridad (a todas les falta algo)

1. un esquema de encripción es seguro si ningún adversario puede encontrar la clave secreta dado un texto cifrado
2. un esquema de encripción es seguro si ningún adversario puede encontrar el texto plano que corresponde con el texto cifrado
3. un esquema de encripción es seguro si ningún adversario puede determinar ningún carácter del texto plano que se corresponde con el texto cifrado.
4. un esquema de encripción es seguro si ningún adversario puede derivar información con significado acerca del texto plano a partir del texto cifrado.

La que sí valdría es:

Un esquema de encripción es seguro si ningún adversario puede calcular ninguna función del texto plano a partir del texto cifrado.
Un esquema criptográfico para una tarea dada es seguro si ningún adversario de poder específico puede lograr un quiebre específico.

Una definición de seguridad debe modelar con precisión el mundo real.

4.2. Principio 2: Dependencia de Suposiciones Precisas.

La mayoría de las construcciones criptográficas modernas no pueden ser probadas como seguras en forma incondicional. Requieren muchas veces resolver cuestiones en la teoria de la complejidad computacional, que aún no tienen respuesta. Por lo tanto hay cuestiones de la seguridad que descansan en algunos supuestos.

Estos supuestos deben ser establecidos con precisión.

1. para dar validez al supuesto
2. para poder comparar esquemas
3. para facilitar pruebas de seguridad

4.3. Principio 3: Pruebas Rigurosas de Seguridad.

Si hay definiciones exactas y suposiciones precisas, es posible una demostración rigurosa de seguridad.

Enfoque reduccionista.

La mayoría de las pruebas de criptografía moderna usan lo que se conoce como el "enfoque reduccionista" Dado un teorema de la forma

"Dado que el supuesto X es verdadero, la construcción Y es segura de acuerdo con la definición dada"

la demostración en general muestra cómo reducir el problema dado por el supuesto X al problema de romper la construcción Y.

La prueba típicamente mostrará cómo un adversario que rompe la construcción Y puede se usado como una subrutina para violar el supuesto X.