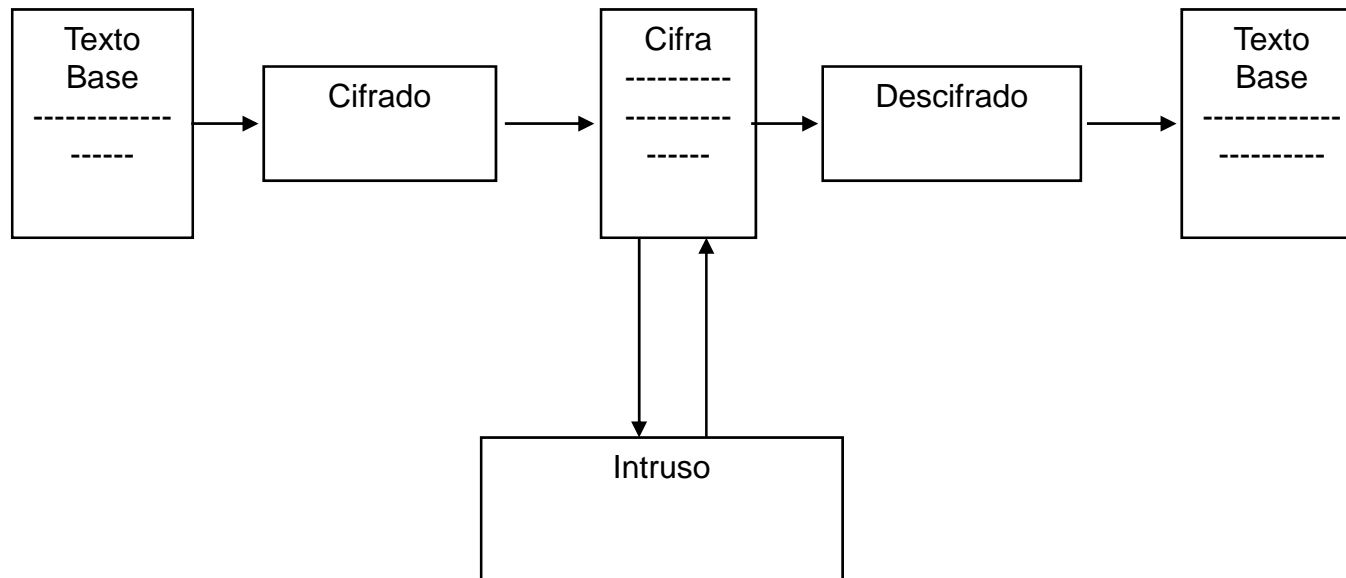


Modelo de comunicación cifrada



Criptografía de clave pública

Terminología

Texto base (B, P): mensaje a cifrar

Texto cifrado (C): resultado del cifrado

Claves (K, K'): cadena alfanumérica usada en el cifrado y descifrado

Notación:

E: algoritmo de cifrado; $C = E[B; K]$

D: algoritmo de descifrado; $B = D[C; K']$

D, E: funciones matemáticas de texto y clave

Propiedad básica: formar un criptosistema: $B = D[E[B; K]; K']$

Fundamentos de un buen método criptográfico: algoritmo de cifrado público y robusto, claves largas (y secretas)

Cuanto más larga es la clave, mayor es el número de intentos necesarios a fuerza bruta

Criptografía de clave secreta

Claves K , K' sólo conocidas por A y B (frecuentemente $K = K'$)

Algoritmos estándar:

DES (Digital Encryption System): IBM-NAS, de 1975 hasta ahora

AES (Advanced Encryption Standard): Rijmen-Daemen, desde ahora

Problema: necesidad de intercambio previo de claves

Requiere contacto físico

Imposible en mundo WWW

Alternativa Diffie-Hellman (1976): criptosistema donde

Clave de cifrado pública; clave de descifrado privada

No derivables una de otra

Criptografía de clave pública I

Esquema: hay un algoritmo de cifrado $E[P; KE]$ y otro de descifrado $D[C; KD]$ sobre claves KE, KD distintas que verifican

1. $D[E[B; KE]; KD] = B$
2. Es muy difícil deducir KD desde E, KE y D
3. D no puede romperse mediante un ataque de texto seleccionado

El primer requisito es imprescindible para la utilidad del sistema

El segundo requisito es obvio

El tercero es fundamental:

Como E y KE son públicos, el atacante puede generar tantos pares (B, C) de texto base y cifrado como quiera

Criptografía de clave pública II

Funcionamiento general: una persona, Ana (A), que quiere recibir mensajes establece dos algoritmos EA, DA, con sus claves KE y KD

A hace públicos EA y KA para que se pueda comunicar con ella

Si otra persona, Benito (B), quiere comunicar un mensaje P a A,

Obtiene EA y KA

Cifra P con EA y KA y obtiene $C = EA[P; KA]$

Envía C a A

Ventaja: posibilidad inmediata de establecer comunicaciones cifradas con cualquier otro usuario del sistema

Inconvenientes: luego!!

¿Cómo llevar a la práctica este esquema?

1ª idea: método de la mochila

2ª idea: método RSA

Método de la mochila I

Primer algoritmo de clave pública; autores: Merkle y Hellman

Idea: problema de la mochila

Se tiene una lista de M objetos O_1, O_2, \dots , de valores V_1, V_2, \dots , y pesos W_1, W_2, \dots , y una mochila que aguanta un peso máximo P

Dado un valor V , se quiere decidir si hay un subconjunto de objetos de peso a lo sumo P y de valor V

Solución muy sencilla, pero coste para M objetos y peso $P = MP = M 2^{\log P}$

=> coste exponencial => cómputo difícil para M, P grandes

No se conocen algoritmos mejores

De hecho la mochila es un problema NP

Método de la mochila II

Variante para Merkle-Hellman: problema de la suma

Se tiene una lista L de M números S_1, S_2, \dots , y un valor V , y se quiere decidir si hay un subconjunto de números cuya suma sea V

Variante de la mochila: pesos iguales a 1, valores S_1, S_2, \dots , y peso máximo M

También es NP

Pero ... ¿cómo usar esto para el cifrado?

Método de la mochila III

B posee una gran lista L de objetos con pesos particulares y distintos, que hace pública => clave = Lista L

Supongamos que la lista es

$$L1 = [575, 436, 1586, 1030, 1921, 569, 721, 1183, 1570]$$

9 elementos => cifrado en bloques de 9 bits

Si A quiere cifrar el bloque 101100111, calcula

$$\begin{aligned} Y &= 575 * 1 + 436 * 0 + 1586 * 1 + 1030 * 1 + 1921 * 0 + \\ & 569 * 0 + 721 * 1 + 1183 * 1 + 1570 * 1 = \\ & 575 + 1586 + 1030 + 721 + 1183 + 1570 = 6665 \end{aligned}$$

B descifra este bloque resolviendo el problema de la suma

Para cada bloque encuentra qué números suman el mensaje

La combinación le da el bloque de texto base

Método de la mochila IV

Enfoque criptográfico: el problema de la suma es NP

Esfuerzo de computación exponencial

Descifrado no factible computacionalmente si listas largas

Consecuencia: el destinatario puede descifrar el mensaje!!

Truco práctico: la lista pública es una variante de una lista

supercreciente: $S_i > S_1 + S_2 + \dots + S_{i-1}$

El problema de la suma es aquí muy fácil

Algoritmo para sucesiones supercrecientes:

si la suma es S su cadena de bits $X_1 \dots X_N$ se obtiene como sigue:

para i de N a 1 :

si $S \geq S_i$: $S = S - S_i$; $X_i = 1$;

else: $i = 0$;

Método de la mochila V

Ejemplo: si la lista es $L2 = [2, 5, 9, 21, 45, 103, 215, 450, 946]$, y $S = 1643$, la evolución es

$$1643 \geq 946 \Rightarrow X9 = 1 \text{ y } 1643 - 946 = 697$$

$$697 \geq 450 \Rightarrow X8 = 1 \text{ y } 697 - 450 = 247$$

$$247 \geq 215 \Rightarrow X7 = 1, \text{ y } 247 - 215 = 32$$

$$32 < 103 \Rightarrow X6 = 0$$

$$32 < 45 \Rightarrow X5 = 0$$

$$32 \geq 21 \Rightarrow X4 = 1, \text{ y } 32 - 21 = 11$$

$$11 \geq 9 \Rightarrow X3 = 1, \text{ y } 11 - 9 = 2$$

$$2 < 5 \Rightarrow X2 = 0$$

$$2 \geq 2 \Rightarrow X1 = 1,$$

que da el texto inicial 1 0 1 1 0 0 1 1 1

Método de la mochila VI

Truco de Merkle: Transformar una sucesión supercreciente L2 en una L1 que no lo es, y de manera invertible

Ejemplo de trap door (puerta trasera): permiten un descifrado fácil a los iniciados

Transformación de sucesión SC a sucesión pública SP: mediante

Módulo $M > SC1 + SC2 + \dots + SCN$,

Multiplicador: P ,

donde $\text{mcd}(P, M) = 1 \Rightarrow$ existe Q tal que $PQ \% M = 1$

Entonces $SP_i = SC_i * P \% M$

Clave pública: SP_1, \dots, SP_N

Clave privada: P , que permite obtener Q y SC_1, \dots, SC_N

Método de la mochila VII

Descifrado: en dos pasos

Multiplicar cada bloque de C por Q módulo M

Resolver problema de la suma supercreciente

Efecto de multiplicar: se obtiene el cifrado equivalente respecto a SC:

Si $C = S_{Pa} + \dots + S_{Pt}$,

$$C * Q \% M = S_{Pa} * Q \% M + \dots + S_{Pt} * Q \% M =$$

$$S_{La} * P * Q \% M + \dots + S_{Lt} * P * Q \% M =$$

$$(S_{La} + \dots + S_{Lt}) * (P * Q \% M) = S_{La} + \dots + S_{Lt}$$

Implementación práctica:

Sucesiones de unos 250 términos

Términos de unos 200 a 400 bits, Multiplicador de unos 200 bits

Método de la mochila VIII

Merkle ofreció 100 dólares a quién pudiera romper el algoritmo en su primera versión

Adi Shamir lo consiguió

Merkle reforzó el algoritmo, ofreciendo ahora 1.000 dólares

Ron Rivest los ganó

Merkle no llegó a ofrecer 10.000 dólares

Leon Adleman se quedó con las ganas

Consecuencias:

El algoritmo de la mochila no se usa,

Pero establece la posibilidad de algoritmos de clave pública

Otros muchos algoritmos se han publicado

El más usado es RSA

RSA I

Descubierto en 1978 por Rivest, Shamir, Adleman, muy amplio uso

Fundamento en teoría de números

Pasos previos al cifrado:

Se escogen dos primos P , Q de más de 100 cifras

Se calculan $N = PQ$, y $Z = (P-1)(Q-1)$

Se escoge un número D primo relativo con Z

Se encuentra un número E con ED congruente con 1 módulo Z

Para cifrar un texto base:

Se divide en bloques B de K bits donde $2^K < N$

=> como un número en base dos, cada bloque B es $<$ que N

B se cifra calculando $C = B^E \pmod{N}$

C se descifra calculando $B = C^D \pmod{N}$

RSA II

El cifrado y el descifrado son inversos uno de otro: pequeño teorema de Fermat

Si M y N son primos relativos, $M^{f(N)} \% N = 1$

con $f(N)$ = función ϕ de Euler = número de enteros $< N$ y primos relativos con N

Entonces:

$$\begin{aligned} C^D \% N &= B^{(ED)} \% N = B^{(1+kZ)} \% N \\ &= B \% N ((B^Z) \% N)^k = B!! \end{aligned}$$

Para el cifrado se necesitan N y E : forman la parte pública

Para el descifrado se necesitan D (y N): forma la parte privada

Seguridad de RSA

Fortaleza de RSA: dificultad de factorizar un número grande

Se conoce N pero no P o Q ; trap door: $N = PQ$

De conocerse:

Z se calcula inmediatamente

D se calcula mediante el algoritmo de Euclides a partir de Z y E

Factorización: problema muy estudiado en Teoría de Números

Más de 300 años y grandes talentos

Problema: si N grande, P y Q son grandes ...

Cómo garantizar en tiempo razonable que son primos?

Solución: usar pseudoprimos

Números de generación “rápida” con muy baja probabilidad de ser compuestos