Criptografía: Seguridad en la información

Guillermo Morales Luna

Sección de Computación
CINVESTAV-IPN

Correo-E: gmorales@cs.cinvestav.mx

Contenido

Resumen

En la actualidad, la gran influencia que las telecomunicaciones tienen en todos los aspectos de la cotidianidad ha hecho que las comunicaciones seguras cobren también particular importancia.
Diferentes enfoques para tratar la seguridad: Aislamiento de los sistemas y entrenamiento a usuarios y administradores de los sistemas de cómputo y de comunicaciones.
Criptografía es la disciplina referente a la construcción de sistemas de cifrado; Criptoanálisis es la disciplina referente al rompimiento de sistemas de cifrado, y Criptología es la conjunción de criptografía y criptoanálisis.
A grandes rasgos, la criptografía puede dividirse en dos tipos: La de llave secreta y la de llave pública. Presentaremos como representante tí pico de llave secreta al sistema DES, asumido por el gobierno de los EUA como un estándar en las tres últimas décadas del siglo pasado. Como representante de llave pública presentamos el método de RSA.

Contenido

Seguridad en la información

La seguridad de la información es vulnerable y susceptible de ataques varios: Errores humanos, empleados incumplidos, empleados desleales, intromisiones externas y factores imponderables tales como incendios o desastres naturales. Para reforzarla se puede asumir diversos enfoques:

- Personal: Accesos mediante tarjetas de control o reconocimiento de rasgos físicos
- Física: Infraestructura de control integral de acceso
- Administrativo: Educación del personal en medidas de seguridad
- Redes de datos: Mediante cifrado y configuraciones de control
- Software y sistemas operativos: Sistemas confiables
- Hardware: Resistencia a intromisiones, cifrado

En todo sistema de seguridad hay que considerar las comunicaciones y los sistemas de cómputo.
Un enfoque muy importante es el cifrado de la información.

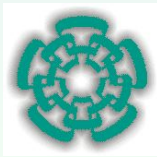
Introducción a la criptografía

La **criptografía** es el estudio de técnicas matemáticas relativas a la seguridad de la información.

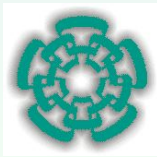
Objetivo. Ofrecer los servicios siguientes:

- Confidencialidad: Mantener la información secreta respecto a quienes no están autorizados a conocerla
- Control de acceso: Restricciones de acceso a ciertos recursos de información permitiendo sólo usuarios distinguidos
- Privacidad: Evitar intromisiones indeseadas a la información propia
- Integridad: Mantener la exactitud de la información, es decir, que no sufra alteraciones por usuarios o medios no-autorizados
- Autentificación de identidades: Reconocimiento de remitentes, corroboración de sus identidades
- Autentificación de mensajes: Reconocimiento de orígenes de la información,

- Anonimato: Reserva de la identidad de una entidad involucrada en un proceso,
- Firmado: Ligamento de partículas de información con entidades
- Sostenimiento de compromisos (Non-repudation): Protección contra actos de desdecirse
- Autorización: Delegación de privilegios a otra entidad para realizar actos propios
- Aval: Otorgamiento temporal de privilegios a otra entidad para realizar actos propios
- Certificación: Respaldo de información por una entidad confiable
- Revocación: Suspensión de certificados o de autorizaciones



- Propiedad: Maneras de otorgar permisos a una entidad para uso o transferencia de recursos
- Testimonio: Verificación de creación o de vigencia de partículas de información por otras partes que los creadores
- Confirmación: Reconocimiento de que ciertos servicios han sido provistos
- Recibo: Acuses de que partículas de información han sido recibidas
- Disponibilidad: Asegurar la entrega oportuna de información
- Fechado o marca de tiempo: Ligamento de partículas de información con momentos de creación o de vigencia



Criptografía (kryptos, griego: Oculto) Disciplina referente a la construcción de sistemas de cifrado.

Criptoanálisis Disciplina referente al rompimiento de sistemas de cifrado.

Criptología Conjunción de la criptografía y el criptoanálisis.

Algo que no es criptografía

En la **esteganografía** (steganos, griego: Cubierto), los mensajes no se transforman mas se ocultan en otro discurso, o bien, se presenta el mensaje con sinónimos:

Lingüística: El caló (jerga de arrabal y albureo). El mensaje simplemente se plantea en vocablos sinónimos o deformados: *Ay nos vidrios en tu cantón, y te caes con la luz*. Otros ejemplos los dan los códigos utilizados en comunicaciones por radio (taxistas, policías, radioaficionados).

Escrita: Los acrósticos o la referencia a símbolos dentro de un texto:

"Un nuevo régimen fiscal para Pemex – Fox anunció en Chile –. El fisco ha de tener ingresos alternativos para obtener si no todas las utilidades actuales, sí lo que compense lo no logrado al hacer más eficiente el gasto público."

si se refiere a los símbolos subrayados

"Un nuevo régimen **f***iscal pa***ra** *Pemex – Fox an***u***nció en Chile – . El fisco ha* **de** *t***en***er ingresos al***t***ernativos pa***r****a*** *o***b***tener si no todas l***as** *utilidades actuales, sí lo que* **co***mpense lo no logrado al hacer más eficiente el gasto público."*

se lee

Fraude en Tabasco

Características criptográficas

Un buen sistema criptográfico ha de tener varias características:

- pequeñas variaciones de textos llanos: grandes variaciones de textos cifrados,
- los tamaños de los textos planos deben ser comparables con los cifrados,
- los textos cifrados deben calcularse eficientemente a partir de los planos, y
- la relación entre textos planos y cifrados debe ser impredecible.

Un mal sistema criptográfico se caracteriza porque:

- aparenta una relación aleatoria entre planos y cifrados, pero en realidad no lo es,
- es susceptible a criptoanálisis elementales,
- el cálculo de cifrados es ineficiente en tiempo y en espacio, y
- es vulnerable a sus propios fabricantes.

Un sistema criptográfico típico de llave secreta consta de los objetos siguientes

- $\mathcal{M}$: un espacio de mensajes,
- $\mathcal{L}$: un espacio de llaves,
- $\mathcal{C}$: un espacio de cifrados de textos,
- $E : \mathcal{L} \times \mathcal{M} \to \mathcal{C}$: función de cifrado,
- $D : \mathcal{L} \times \mathcal{C} \to \mathcal{M}$: función de descifrado, tales que
  - $\forall k \in \mathcal{L}, m \in \mathcal{M} : \ D(k, E(k, m)) = m$ &
  - $\forall k \in \mathcal{L}, c \in \mathcal{C} : \ E(k, D(k, c)) = c$.

El sistema es seguro si a pesar de conocer $E(k, m)$, desconociendo k no se puede calcular m.

Ejemplo

Rellenado de una sola vez (one-time pad)

En $\mathbb{Z}_2$ la operación suma $\oplus$, u "O"-excluyente, es de orden 2: $x \oplus x = 0$, y $\forall n \in \mathbb{N}$, la misma operación componente a componente cumple lo mismo: $\forall \mathbf{x} \in \mathbb{Z}_2^n : \ \mathbf{x} \oplus \mathbf{x} = \mathbf{0}$. Así pues, se puede tomar $\mathcal{M} = \mathcal{L} = \mathcal{C} = \mathbb{Z}_2^n$ y

$$\begin{array}{rcl} E : \mathcal{L} \times \mathcal{M} & \rightarrow & \mathcal{C} \\ (\mathbf{k}, \mathbf{m}) & \mapsto & \mathbf{c} = \mathbf{k} \oplus \mathbf{m} \end{array} \qquad \begin{array}{rcl} D : \mathcal{L} \times \mathcal{C} & \rightarrow & \mathcal{M} \\ (\mathbf{k}, \mathbf{c}) & \mapsto & \mathbf{m} = \mathbf{k} \oplus \mathbf{c} \end{array}$$

el sistema es seguro pues conocido $\mathbf{c}$ si no se conoce $\mathbf{k}$ no es recuperable $\mathbf{m}$ (de hecho, es posible generar cualquier $\mathbf{m}$ pues siempre existe $\mathbf{k} = \mathbf{m} \oplus \mathbf{c}$ tal que $\mathbf{m} = D(\mathbf{k}, \mathbf{c})$.

Ejemplo

Transformaciones lineales no-singulares

Sea $\mathbf{A} \in (\mathbb{Z}_2)^{n \times n}$ una matriz tal que $\mathrm{Det}\ \mathbf{A} \neq 0$ y sea $\mathbf{b} \in \mathbb{Z}_2^n$. Entonces la pareja $(\mathbf{A}, \mathbf{b})$, que contiene $n^2 + n$ "entradas" en $\mathbb{Z}_2$, determina una transformación afín

$$T_{(\mathbf{A},\mathbf{b})} : \mathbf{m} \mapsto \mathbf{Am} + \mathbf{b}$$

con inversa $T^{-1}_{(\mathbf{A},\mathbf{b})} = T_{(\mathbf{A}^{-1},\mathbf{0})} \circ t_{-\mathbf{b}}$, donde $t_{-\mathbf{b}}$ es la translación $\mathbf{x} \mapsto \mathbf{x} - \mathbf{b}$.

Cifrado por bloques

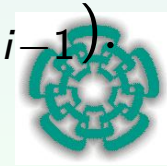
Dado un mensaje $\mathbf{m} = (a_i)_{i \leq m}$, se parte en bloques $\mathbf{m}_i = \left(a_{(i-1)k+j}\right)_{j \leq k}$, donde $k|n$. Se cifra cada bloque para obtener el cifrado $\mathbf{c}_i = E_{Llave}(\mathbf{m}_i)$ y el cifrado de todo el mensaje es: $\mathbf{c} = (\mathbf{c}_i)_{i \leq \frac{m}{k}}$.

Dos tipos de cifrado de bloques.

De ráfaga

En cada bloque i se usa una llave distinta y los cifrados anteriores: $\mathbf{c}_i = E_{i,Llave_i}(\mathbf{m}_i, \mathbf{c}_{i-1})$. Permite bloques pequeños. Hay varios modos de operación:

1. Cipher block chaining mode (CBC) Se toma como E_{Llave} una permutación y $\mathbf{c}_i = E_{Llave}(\mathbf{m}_i \oplus \mathbf{c}_{i-1})$ donde $\mathbf{c}_0$ es un texto inicial. El mensaje se recupera haciendo $\mathbf{m}_i = D_{Llave}(\mathbf{c}_i \oplus \mathbf{c}_{i-1})$ con $D_{Llave} = E^{-1}_{Llave}$.
2. Output feedback mode (OFB) Se toma como E_{Llave} una permutación (la llave se mantiene constante) y se hace $\mathbf{v}_i = E_{Llave}(\mathbf{v}_{i-1})$, $\mathbf{c}_i = E_{Llave}(\mathbf{m}_i \oplus \mathbf{v}_i)$ donde $\mathbf{v}_0$ es una semilla inicial. El mensaje se recupera haciendo $\mathbf{m}_i = D_{Llave}(\mathbf{c}_i \oplus \mathbf{v}_i)$.
3. Cipher feedback mode (OFB), $\mathbf{c}_i = \mathbf{m}_i \oplus E_{Llave}(\mathbf{c}_{i-1})$ donde $\mathbf{c}_0$ es un texto inicial. El mensaje se recupera haciendo $\mathbf{m}_i = \mathbf{c}_i \oplus E_{Llave}(\mathbf{c}_{i-1})$.



Uniforme

En cada bloque i se utiliza una misma función y una misma llave: $\mathbf{c}_i = E_{Llave}(\mathbf{m}_i)$. Aquí se tiene el modo de código de libro electrónico (electronic code book mode (ECB)). La característica principal es que:

$$\forall i, j: \quad \mathbf{c}_i = \mathbf{c}_j \;\Leftrightarrow\; \mathbf{m}_i = \mathbf{m}_j.$$

Contenido

Data Encryption Standard (DES)

El estándar de cifrado de datos, Data Encryption Standard (DES), ha sido de los más utilizados en la historia de la criptografía:

- Se desarrolló en los años 70, por IBM, principalmente.
- En 1977 se adoptó como un estándar por la Oficina Nacional de Estándares (NBS: National Bureau of Standards, en la actualidad el National Institute of Standards and Technology) del Gobierno de los EUA.
- Es de cifrado por bloques, con bloques de 64 bits.
- Utiliza llaves de 56 bits (dadas en 8 bytes, en cada uno de los cuales 7 bits son de la llave y el octavo es de paridad).
- Consecuentemente, el espacio de búsqueda para la llave es de tamaño 2^{56} (en promedio se requiere de 2^{55} pasos de búsqueda).
- El cifrado se hace con 16 ciclos de reiteración. En cada ciclo, los paraámetros de la función de cifrado dependen de los bloques de datos y de llaves, actuales y previos.
- En cada ciclo, la (sub-)llave $Llave_i$, $i = 1, \ldots, 16$ se construye mediante un algoritmo de preparación de llaves (key scheduling

Dado un mensaje $\mathbf{m} = \mathbf{m}_{Izq}\mathbf{m}_{Der}$ de 64 bits, es decir, 8 bytes, $\mathbf{m}_{Izq}, \mathbf{m}_{Der}$ de 4 bytes cada uno, se procede como sigue:

1. Sea $\mathbf{m}_{Izq}^{(1)}\mathbf{m}_{Der}^{(1)} = \mathbf{m}^{(1)} = T(\mathbf{m})$, donde T es una permutación.
2. Para $i = 2, \ldots, 16$ hágase

$$\begin{aligned} \mathbf{m}_{Izq}^{(i)} &= \mathbf{m}_{Der}^{(i-1)} \\ \mathbf{m}_{Der}^{(i)} &= \mathbf{m}_{Izq}^{(i-1)} \oplus f\left(\mathbf{m}_{Der}^{(i-1)}, Llave_i\right) \end{aligned}$$

   donde $Llave_i$ tiene una longitud de 48 bits.
3. $\mathbf{c} = T^{-1}(\mathbf{m}_{Izq}^{(16)}\mathbf{m}_{Der}^{(16)})$.

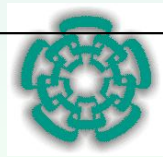
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Permutación inicial T.

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Permutación inversa T^{-1}.

Cada permutación se presenta como una matriz $\mathbf{A} \in [\![1, 64]\!]^{8\times 8}$. Si $\mathbf{m} = \left[m_{8(i-1)+j}\right]_{i=1,\ldots,8}^{j=1,\ldots,8} \in \mathbb{Z}_2^{64}$ es una cadena de 64 bits, entonces $A(\mathbf{m}) = \left[n_{8(i-1)+j} = m_{A_{ij}}\right]_{i=1,\ldots,8}^{j=1,\ldots,8}$.



El cálculo de $f : \mathbb{Z}_2^{32} \times \mathbb{Z}_2^{48} \rightarrow \mathbb{Z}_2^{32}$, $(\mathbf{m}_{Der}, Llave_i) \mapsto f\,(\mathbf{m}_{Der}, Llave_i)$ utiliza 8 transformaciones $S_j : \mathbb{Z}_2^6 \rightarrow \mathbb{Z}_2^4$, $j = 1, \ldots, 8$, llamadas S-cajas, **fijadas de antemano por los estándares**.

Cada S-caja se especifica como una matriz $\mathbf{S} \in [\![1, 16]\!]^{4\times 16}$. Para una cadena de 6 bits $\mathbf{r} = r_1 r_2 r_3 r_4 r_5 r_6$, $S(\mathbf{r})$ es la escritura en binario (con 4 bits) del número $\mathbf{S}_{ij}$, donde $i = 2r_1 + r_6$ y $j = (r_2 r_3 r_4 r_5)_2$.

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

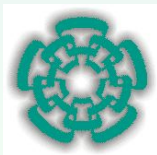
S-caja S_1

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S-caja S_2

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S-caja S_3



7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

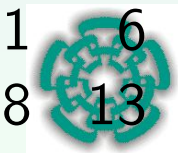
S-caja S_4

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S-caja S_5

12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S-caja S_6

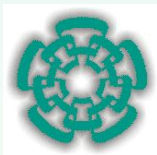


4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S-caja S_7

13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

S-caja S_8



f se calcula como sigue:

1. Duplicando bits en 16 posiciones, la cadena $\mathbf{m}_{Der}$ de 32 bits se expande a una cadena $\mathbf{m}'_{Der}$ de 48 bits. Precisamente, se aplica la función $E : \mathbb{Z}_2^{32} \rightarrow \mathbb{Z}_2^{48}$ descrita adelante.
2. Sea $\mathbf{r} = \mathbf{m}'_{Der} \oplus Llave_i \in \mathbb{Z}_2^{48}$.
3. Escríbase $\mathbf{r} = [\mathbf{r}_j]_{j=1}^{8}$, donde cada $\mathbf{r}_j \in \mathbb{Z}_2^6$ es una cadena de 6 bits.
4. Hágase $f\left(\mathbf{m}_{Der}^{(i-1)}, Llave_i\right) = P\left[S_j\left(\mathbf{r}_j\right)\right]_{j=1}^{4} P\left[S_j\left(\mathbf{r}_j\right)\right]_{j=5}^{8}$, donde P es una permutación $\mathbb{Z}_2^{32} \rightarrow \mathbb{Z}_2^{32}$.

La expansión se da como una matriz $\mathbf{E} \in [\![1, 32]\!]^{8\times 6}$. Si $\mathbf{m} = \left[m_{4(i-1)+j}\right]_{i=1,\ldots,8}^{j=1,\ldots,4} \in \mathbb{Z}_2^{32}$ es una cadena de 32 bits, entonces $E(\mathbf{m}) = \left[n_{6(i-1)+j} = m_{E_{ij}}\right]_{i=1,\ldots,8}^{j=1,\ldots,6}$.

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

La permutación se presenta como una matriz $\mathbf{P} \in [\![1, 32]\!]^{8\times 4}$. Si $\mathbf{m} = \left[m_{4(i-1)+j}\right]_{i=1,\ldots,8}^{j=1,\ldots,4} \in \mathbb{Z}_2^{32}$ es una cadena de 32 bits, entonces $P(\mathbf{m}) = \left[n_{4(i-1)+j} = m_{P_{ij}}\right]_{i=1,\ldots,8}^{j=1,\ldots,4}$.

En cuanto a la generación de sub-llaves,
dada la llave del usuario de 56 bits, primero se transpone a sus bits, y se fracciona en dos partes de 28 bits cada una.
Se va rotando a estas partes uno o dos bits a la izquierda, dependiendo del índice del ciclo, y de acuerdo con una regla fija, se compone a las partes para producir la llave $Llave_i$ de 48 bits.
Puesto con más precisión:

1. Sea $Llave = [k_i]_{i=1}^{64}$ una llave dada en 8 bytes, es decir, 64 bits. Los bits k_{8i}, $i = 1, \ldots, 8$ son de paridad. Se les descarta y los restantes forman la llave de 56 bits propia del usuario.
2. Sea $L = \mathbf{P}_1(Llave)$ la cadena de 56 bits formada mediante la matriz $\mathbf{P}_1$, aplicada a $Llave$. Escríbasela como la concatenación de dos cadenas de 28 bits cada una, $[C_0, D_0] = L$.
3. Para cada ciclo $i \leq 16$, hágase $v_i = \begin{cases} 1 & \text{si } i \in \{1, 2, 9, 16\}, \\ 2 & \text{en otro caso.} \end{cases}$

   En otras palabras, de acuerdo con el índice de cada ciclo se ha de rotar como se indica a continuación:

Ciclo i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Rotaciones v_i	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

   Sea $\gamma : \mathbb{Z}_2^{28} \to \mathbb{Z}_2^{28}$ la rotación consistente de "correr un lugar hacia la izquierda" cada uno de los 28 bits.
4. Para cada $i = 2, \ldots, 16$ hágase $C_i = \gamma^{v_i}(C_{i-1})$, $D_i = \gamma^{v_i}(D_{i-1})$ y sea $Llave_i = \mathbf{P}_2([C_i, D_i])$ la llave de 48 bits formada mediante la matriz $\mathbf{P}_2$.

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Para formar una cadena L de 56 bits a partir de una K de 64 bits, se toma en la posición $8(i-1)+j$ de L, $1 \leq i \leq 8$, $1 \leq j \leq 7$, al bit $(\mathbf{P}_1)_{ij}$-ésimo de K.

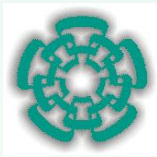
Para formar una llave K de 48 bits a partir de una cadena L de 56 bits, se toma en la posición $8(i-1)+j$ de K, $1 \leq i \leq 8$, $1 \leq j \leq 6$, al bit $(\mathbf{P}_2)_{ij}$-ésimo de L.

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Para descifrar se sigue el mismo procedimiento, en sentido inverso.

Observaciones:

- Las S-cajas definen transformaciones que no son lineales ni afines. En tanto sean más complejas, la seguridad será mayor.
- Una llave es débil si $E_{Llave}(E_{Llave}(\mathbf{m})) = \mathbf{m}$.
- **Propiedad de complemento.** $\mathbf{c} = E_{Llave}(\mathbf{m}) \implies \overline{\mathbf{c}} = E_{\overline{Llave}}(\overline{\mathbf{m}})$.
- En la actualidad, la llave resulta pequeña.
- La implementación en hardware de las S-cajas es propiedad de IBM y no se publicó su diseño, lo cual conlleva vulnerabilidad.



Un posible ataque:

1. Escójase $\mathbf{m}$.
2. Obténgase los cifrados de $\mathbf{m}$ y $\overline{\mathbf{m}}$: $\mathbf{c}_0 = E_{Llave}(\mathbf{m})$ y $\mathbf{c}_1 = E_{Llave}(\overline{\mathbf{m}})$.
3. Para las 2^{55} llaves $Llave'$ cuyo bit más significativo es 0, revísese si $E_{Llave'}(\mathbf{m}) \in \{\mathbf{c}_0, \mathbf{c}_1\}$. En tal caso, se tendrá evidencia de que $Llave = Llave'$ si $E_{Llave'}(\mathbf{m}) = \mathbf{c}_0$ o bien de que $Llave = \overline{Llave'}$ si $E_{Llave'}(\mathbf{m}) = \mathbf{c}_1$.

Triple DES

Como un reforzamiento de DES, Triple DES aplica tres veces el método convencional DES para obtener un cifrado final de cada mensaje. Sea $DES : (Llave, \mathbf{m}) \mapsto \mathbf{c}$ la función de cifrado descrita anteriormente. Escribamos

$$DES_{Llave} : \mathbf{m} \mapsto DES(Llave, \mathbf{m}).$$

Llaves de 168 bits Dadas tres llaves $Llave_1, Llave_2, Llave_3$ de 56 bits cada una (juntas por tanto dan 168 bits) se hace, para cada mensaje $\mathbf{m}$:

$$\mathbf{c} = DES_{Llave_3} \circ DES^{-1}_{Llave_2} \circ DES_{Llave_1}(\mathbf{m})$$

Llaves de 112 bits Dadas dos llaves $Llave_1, Llave_2$ de 56 bits cada una (juntas por tanto dan 112 bits) se hace, para cada mensaje $\mathbf{m}$:

$$\mathbf{c} = DES_{Llave_1} \circ DES^{-1}_{Llave_2} \circ DES_{Llave_1}(\mathbf{m})$$

En cualquier caso, se puede utilizar cualesquiera de los modos ECB, CBC, OFB y CFB.

Contenido

Métodos de llave pública

En este esquema cada usuario tiene un "buzón, con una ranura de entrada: cualquier otro usuario sabe cómo meter un mensaje en ese buzón, mas sólo el dueño del buzón puede extraer mensajes". El término inglés trapdoor one-way denota precisamente esta idea: Un ratón puede entrar con facilidad a una trampa mas de ella no puede salir. Utilizaremos, con todas las reservas del caso, el término unidireccional para referirnos a one-way.
En todo esquema de llave pública cualquier usuario U posee dos llaves (e_U, d_U). Cuando un usuario V ha de enviar un mensaje m a U, calcula un código $c = f(m, e_U)$ utilizando la llave pública de U. U descifra el mensaje calculando $m = g(c, d_U)$ utilizando su propia llave secreta d_U.
Así pues la llave secreta de U está en función de su llave pública e_U.
Naturalmente, d_U no ha de ser calculable sólo a partir de e_U. Por otro lado, las funciones f y g, que guardan cierta relación de inversibilidad, una respecto a la otra, han de ser funciones de iguales complejidades.
En la actualidad, RSA es el prototípico esquema de llave pública. Veremos en esta lección algunos otros esquemas de llave pública.

Teorema (Pequeño de Fermat)

Si p es primo y $a \in \mathbb{N}$ no es divisible entre p, entonces $a^{p-1} \bmod p = 1$.

Sean p, q dos números primos, y sea $n = p \cdot q$ su producto. Por el teorema de Fermat, se tiene que para cualquier $x \neq 0$,

$$x^{p-1} \bmod p = 1 \qquad \text{y} \qquad x^{q-1} \bmod q = 1,$$

consecuentemente

$$x^{(p-1)(q-1)} \bmod p = 1 \qquad \text{y} \qquad x^{(p-1)(q-1)} \bmod q = 1.$$

Es decir

$$p \left| (x^{(p-1)(q-1)} - 1) \right. \qquad \text{y} \qquad q \left| (x^{(p-1)(q-1)} - 1) \right. .$$

Así pues, $n \left| (x^{(p-1)(q-1)} - 1) \right.$. Es decir, $\boxed{x^{(p-1)(q-1)} \bmod n = 1}$.

Función de Euler

$$\phi : n \mapsto \text{card}\{m \leq n | m \text{ es primo relativo con } n\}.$$

Entre las propiedades más importantes de esta función están:

- Si p es primo, entonces $\phi(p) = p - 1$.
- ϕ es multiplicativa, es decir, si m y n son primos relativos entonces $\phi(mn) = \phi(m)\phi(n)$.
- Si p es primo y $r \in \mathbb{N}$, entonces $\phi(p^r) = p^{r-1}(p-1)$.
- $\limsup_{n \to +\infty} \dfrac{\phi(n)}{n} = 1$.
- $\liminf_{n \to +\infty} \dfrac{\phi(n)\ln(\ln(n))}{n} = e^{-\gamma}$, donde $\gamma = 0.577215\ldots$ es la, así llamada, constante de Euler.

Teorema (Pequeño de Fermat (bis))

Si n es un entero no-nulo y $a \in \mathbb{N}$ es primo relativo con n, entonces $a^{\phi(n)} \bmod n = 1$.

Además, dado que la función "módulo" es un homomorfismo, se tiene

$$r \bmod \phi(n) = s \;\Rightarrow\; a^r \bmod n = a^s.$$

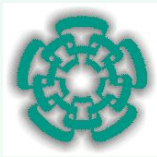
Consecuentemente, si e, d son enteros tales que
$e \cdot d \bmod (p-1)(q-1) = 1$ se tiene que: $a^{ed} \bmod n = a$.
Esta es la base del algoritmo de cifrado: Si a es el mensaje, se hace $c = a^c$ su cifrado. Entonces, $c^d = m$.
La pareja (n, e) es la llave, que puede hacerse pública.
La llave secreta es (n, d).
Para calcular d sabiendo e, es necesario conocer la factorización de n como producto de los dos primos p y q.

Cifrado

De manera aún más restringida, si p y q son primos, $n = pq$ y $\lambda(n) = \text{m.c.m.}(p-1, q-1)$ entonces también vale

$$e \cdot d \bmod \lambda(n) = 1 \;\Rightarrow\; a^{ed} \bmod n = a.$$

Observamos que si se conoce p, q, entonces dado e se calcula, mediante el Algoritmo de Euclides para el Cálculo del Máximo Común Divisor, a su inverso multiplicativo d en el anillo $\mathbb{Z}^*_{\text{m.c.m.}(p-1,q-1)}$.
Cualquier ataque contra el sistema de cifrado tiene como objetivo calcular d.



Entrada:
Un mensaje $m < n$
La llave pública (n, e).
Salida:
El cifrado c.

`Cifrar`
$\{ \quad c := m^e \bmod n$
$\}$

Entrada:
Un cifrado $c < n$
La llave privada (n, d).
Salida:
El mensaje m.

`Descifrar`
$\{ \quad m := c^d \bmod n$
$\}$

Ejemplo

Consideremos dos primos grandes: $p = P_{23007} = 262231$ y $q = P_{23008} = 262237$. Su producto es entonces $n = pq = 68766670747$ el cual número se escribe con un número de bits igual a $\lfloor \log_2 n \rfloor + 1 = 37$. Si se toma el exponente $e = 12521$ se tiene que e es primo relativo con el mínimo común múltiplo de $p - 1$ y $q - 1$. Sea $\lambda = \text{m.c.m.}(p - 1, q - 1) = 11461024380$. De hecho, se tiene $1 = d \cdot e + k \cdot \lambda$, donde $d = 1132280741$ y $k = -1237$.
Para un valor como $m = 1562435$ el código correspondiente es

$$c = m^e \bmod n = 56009798215$$

y, en efecto, si calculamos la potencia correspondiente al exponente d,

$$m' = c^d \bmod n = 1562435,$$

vemos que ésta coincide con el mensaje original m.

Ejemplo

Como un segundo ejemplo, consideremos la cadena de caracteres

Mexicanos al grito de guerra

al tomar uno a uno los caracteres

M , e , x , i , c , a , n , o , s , , a , l , , g , r , i , t , o , , d , e , , g , u , e , r , r , a

y al ponerlos en código ASCII, obtenemos la sucesión de números

77, 101, 120, 105, 99, 97, 110, 111, 115, 32, 97, 108, 32, 103, 114, 105, 116, 111, 32, 100, 101, 32, 103, 117, 101, 114, 114, 97

Al tomarlos de cuatro en cuatro, cada tira de cuatro números se interpreta como un entero, entre 0 y $256^4 - 1$, escrito en base 256. Aplicamos pues una conversión de base 256 a base 10. Los 28 caracteres dan 7 números:

1298495593 1667329647 1931501932 543650409
1953439844 1696622453 1701999201

Aplicamos a cada uno la función de cifrado:

63933001817 25675825739 5190155225 15978589175 28389357636 1

y al aplicar la función de reconversión a base 256

226, 180, 48, 89, 250, 102, 2, 75, 53, 91, 123, 217, 184, 101, 235, 247, 156, 35, 56, 68, 110, 165, 72, 237, 149, 9, 131, 238

que son códigos correspondientes a los caracteres

â , ′ , 0 , Y , ú , f , ⟨no-imprimible⟩ , K , 5 , [, { , Ù , ∠ , e , ë , ÷ , ⟨no-imprimible⟩ , # , 8 , D , n , ¥ , H , í , ⟨no-imprimible⟩ , , ⟨no-imprimible⟩ , î

algunos de los cuales no son imprimibles. La cadena yuxtapuesta es

â′0Yúf⟨no-imprimible⟩K5[{Ù∠eë÷⟨no-imprimible⟩#8Dn¥Hí⟨no-imprimible⟩⟨no-imprimible⟩î

Ahora procediendo en sentido inverso, partiendo de

63933001817 25675825739 5190155225 15978589175
28389357636 14741227757 32565199854

calculamos la función de descifrado, para obtener

1298495593 1667329647 1931501932 543650409
1953439844 1696622453 1701999201

la cual sucesión efectivamente coincide con la "original"

1298495593 1667329647 1931501932 543650409
1953439844 1696622453 1701999201

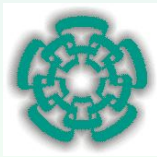
Contenido

Internet y seguridad

A principios de 1970, el ejército de Estados Unidos, bajo la agencia militar DARPA (Defense Advanced Research Projects Agency), actualmente conocida con el nombre ARPA, estableció un financiamiento para desarrollar la red de datos ARPANet, la cual interconectaba a diversas universidades norteamericanas y centros de investigación. Internet aparece en 1980, y comienza a integrar las máquinas conectadas a su red de investigación para usar los nuevos protocolos de TCP/IP. La transición se terminó en enero de 1983, cuando ARPANet establece como obligatorio el uso de TCP/IP en todas las computadoras conectadas a ésta.

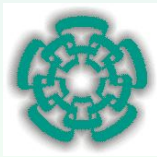
IETF

El organismo Internet Engineering Task Force, es el grupo más importante de Internet en cuanto a su desarrollo tecnológico. Este constituye una gran comunidad internacional de red, integrada por diseñadores, operadores, vendedores e investigadores, todos ellos preocupados por la evolución y la operación de Internet. El foro de IETF [5] está abierto a cualquier interés individual.



Documentos Internet y estándares

Las propuestas para estándares Internet pueden ser encontradas en dos tipos de documentos: Internet Drafts (IDs) y Requests for Comments (RFCs). Los Internet Drafts no son documentos formales y pueden ser cambiados o eliminados en cualquier momento. Los RFCs son la serie oficial de documentos del IAB, y los cuales son almacenados permanentemente, y nunca son borrados; una vez que un RFC es publicado, nunca cambiará. La mayoría de estos documentos son localizados en línea en forma de actas de la IEFT.



S/MIME y OPEN PGP

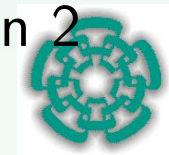
Los servicios de seguridad pueden ser agregados a cada enlace de comunicación a lo largo de una trayectoria dada, o pueden ser integrados alrededor de los datos que están siendo enviados, siendo esto independiente de los mecanismos de comunicación. Este enfoque avanzado es frecuentemente llamado seguridad "nodo-a-nodo" (end-to-end). Existen dos propuestas principales para ofrecer los servicios de seguridad que hemos mencionado: S/MIME y PGP. Otros protocolos han sido propuestos en el pasado como son PEM y MOSS, no tuvieron mayor presencia. Sin embargo, ahora diversos proveedores de servidores de correo electrónico, incluyen en sus productos a S/MIME, PGP/MIME y OpenPGP.

S/MIME fue desarrollado por RSA Data Security, Inc. Se establece en el formato PKCS #7 para los mensajes, y en el formato X.509v3 para los certificados. PKCS #7 se basa en el formato ASN.1 DER para datos.
PGP/MIME, toma como base a PGP, el cual se había desarrollado por diversos investigadores, algunos de los cuales formaron a la compañia PGP, Inc. Los formatos tanto para mensajes como para certificados, fueron creados de improvisar y usar una simple codificación binaria. OpenPGP se funda en PGP.
S/MIME, PGP/MIME, y OpenPGP usan MIME para estructurar sus mensajes. Los esquemas antes mencionados tienen confianza en el tipo MIME multipart/signed, el cual se describe en el RFC 1847 para mover mensajes firmados sobre Internet. Un cliente de correo puede razonablemente aceptar y enviar ambos formatos.

S/MIME es un protocolo nuevo, con una versión inicial desarrollada por un consorcio privado de compañias. S/MIME ha conseguido amplia adopción en la industria de correo de Internet. La mayoría ha creado su programas de correo usando varios drafts del protocolo S/MIME v2 que han estado circulando en el IETF. Las partes del protocolo son:

- S/MIME Version 2 Message Specification (RFC 2311)
- S/MIME Version 2 Certificate Handling (RFC 2312)
- PKCS #1: RSA Encryption Version 1.5 (RFC 2313)
- PKCS #10: Certification Request Syntax Version 1.5 (RFC 2314)
- PKCS #7: Cryptographic Message Syntax Version 1.5 (RFC 2315)
- Description of the RC2 Encryption Algorithm (RFC 2268)

Estos RFCs, tienen el carácter de informativos. Es importante notar que S/MIME v2 no es un estándar del IETF. S/MIME requiere el uso de una llave de intercambio RSA, lo que es gravado por las patentes americanas influenciado por RSA Data Security, Inc, lo que favorece que la versión 2 de S/MIME requiera el uso de criptografía débil (llaves de bits).



Contenido

Bibliografía

- F. Bauer. Decrypted secrets: Methods and maxims of cryptology, Springer, 2000.
- G. Brassard. Modern Cryptology. Volume 325 of Lecture Notes in Computer Science, Springer-Verlag, 1988.
- D. E. Comer, Internetworking with TCP/IP, Volume I, Principles, Protocols and Architecture, Prentice-Hall, 3rd edition, 1995.
- W. Diffie and M.E. Hellman. New directions in cryptography. IEEE Transactions on Information Theory, IT-22: 644-654, 1976.
- Internet Engineering Task Force, `http://www.ietf.org`
- D. Kahn. The Codebreakers. Macmillan Co., New York, 1967.
- N. Koblitz. A Course in Number Theory and Cryptography. Springer-Verlag, 1994.

- A.J. Menezes, P.C. van Oorschot, S.A. Vanstone. Handbook of Applied Cryptography, CRC Press, 1996. http://www.cacr.math.uwaterloo.ca/hac/index.html
- R. Rivest. Cryptography, J. van Leeuwen, editor, Handbook of Theoretical Computer Science, 719-755, Elsevier Science Publishers, 1990.
- RSA Laboratories, Frequently Asked Questions About Today's Cryptography. http://www.rsasecurity.com
- B. Schneier. Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley & Sons, New York, 2nd edition, 1996.
- G.J. Simmons, editor. Contemporary Cryptology: The Science of Information Integrity. IEEE Press, 1992.
- D. R. Stinson. Cryptography: Theory and Practice, CRC Press, 1995.