Universidad Rey Juan Carlos

Grado en Ingeniería de la Ciberseguridad

Criptografía

Sesión 4. Cifrado Asimétrico.

---

1. Considera que Alice y Bob establecen una clave con el intercambio de Diffie-Hellman en $\mathbb{Z}_{17}^*$ tomando como generador $g = 3$. Alice envía un 12, mientras que Bob envía un 14. ¿Puedes obtener (por fuerza bruta) la clave que Alice y Bob han establecido?

2. Considerar un esquema RSA con clave pública $N = 187, e = 7$. Descifra el texto $C = 13$ (puedes dejar el resultado indicado sin terminar las cuentas).

3. Dado un esquema RSA con clave pública $N = 55, e = 7$, cifra el mensaje $M = 12$, encuentra p, q, d y descifra $c = 37$ (puedes dejar el resultado indicado sin terminar las cuentas).

4. Supongamos que un adversario que ataca el criptosistema RSA es capaz de calcular la función de Euler del módulo, $\varphi(N)$. ¿A qué tiene acceso?

5. Considera que hay dos ususarios del sistema, Bob y Berto, que tienen claves públicas RSA con el mismo módulo N pero distintos exponentes e_1 y e_2.

   a) Demuestra que Bob puede descifrar mensajes enviados a Berto

   b) Demuestra que un adversario es capaz de descifrar cualquier mensaje que se haya enviado a la vez a Bob y a Berto, si $m.c.d.(e_1, e_2) = 1$

6. Considera una modificación del esquema de cifrado de Bellare y Rogaway en la que el cifrado de un texto m conste de tres componentes:

   - $f(r)$, con r aleatorio y f una función *one-way*,
   - $m \cdot f(r)$,
   - $H(r)$, con H un oráculo aleatorio

   Analiza informalmente la seguridad del esquema resultante.

Recordad:

Esta hoja se corresponde con ejercicios de clase MAGISTRAL, grupos separados. Algunos, por tanto, son ejercicios difíciles que no podréis resolver solos por vuestra cuenta.

Importante

→ ¡Intentadlos! A ver hasta dónde elegáis

→ ¡Entended la solución!

→ ¡Preguntad!

1| $G = \mathbb{Z}_{17}^* = \{\cancel{0}, 1, \ldots, 16\}$

$g = 3$

Alice envía 12; busquemos a t.q. $g^a \equiv 12 \mod 17$.

Bob envía 14; " b t.q. $g^b \equiv 14 \mod 17$

Lo haremos por fuerza bruta, calculando todas las potencias de g (mod 17)

$g^0 \equiv 1$

$g^1 \equiv 3$

$g^2 \equiv 9$

$g^3 \equiv 27 \equiv 10$

$g^4 \equiv 30 \equiv 13$ (×3)

$g^5 \equiv 39 \equiv 5$ (×3)

$g^6 \equiv 15$ (×3)

$g^7 \equiv 45 \equiv 11$ (×3)

$g^8 \equiv 33 \equiv 16$ (×3)

$g^9 \equiv 14$

$g^{10} \equiv 8$

$g^{11} \equiv 7$

$g^{12} \equiv 4$

$g^{13} \equiv 12$

(no seguimos!)

Así $a = 13$, $b = 9$ y la clave $K = g^{ab} \mod 17$

$= 3^{117} \mod 17$

Recordad que

$$g^{\alpha} \equiv g^{\beta} \mod p$$

$$\iff \alpha \equiv \beta \mod p-1$$

luego sustituid 117 por $117 \bmod 16 = 5$

y $K = g^5 = 5$ —

2] $N = 187$

$e = 7$

Tenemos que descifrar $C = 13$, luego necesitamos:

1 - Factorizar N (Encontrar p y q con $N = p \cdot q$)

2 - Calcular $\varphi(N)$ ($(p-1)(q-1)$)

3 - Calcular $d = e^{-1} \bmod \varphi(N)$

4 - Descifrar haciendo $m = C^d \bmod N$.

1] $187 = 11 \times 17$ (hemos probado y no es divisible por 2, 3, 5, 7...).

2] $\varphi(N) = 10 \times 16 = 160$.

3] ¡Usamos lo aprendido en disctas! Algoritmo de Euclides + Identidad de Bezout:

Como $1 = mcd(e, \varphi(N))$, buscamos enteros α y β tales que

$$\alpha e + \beta \varphi(N) = 1$$

luego

$$e^{-1} = d \equiv \alpha \bmod \varphi(N)$$

$1 = mcd(160, 7) = mcd(7, 6) = mcd(6, 1) = 1$

$160 = 22 \times 7 + 6 \Rightarrow$ $6 = 160 - 22 \times 7$

$7 = 6 \times 1 + 1$ ← mcd $\Rightarrow$ $1 = 7 - 6 \times 1$.

$6 = 6 \times 1 + 0$

$$1 = 7 - (160 - 22 \times 7) = \underbrace{23}_{\alpha} \times \underbrace{7}_{e} + \underbrace{(-1)}_{\beta} \underbrace{160}_{\varphi(N)}$$

Así, $e^{-1} \equiv 23 \bmod 160 \Rightarrow e^{-1} = d = 23$

4] ¡Desciframos!

$m \equiv 13^{23} \mod 187$ ← hasta aquí es suficiente ✓

$\equiv 140$

3] RSA $N = 55$, $e = 7$, $M = 12$,

$N = 55 = 5 \times 11$, luego $p = 5$, $q = 11$ (o al revés, ☺)

$\varphi(N) = 4 \times 10 = 40$;

i) Ciframos $M = 12$ haciendo $C^* \equiv 12^7 \mod 55$

ii) Encontramos, como en el ejercicio anterior, $d \equiv e^{-1}$ y desciframos

i) $C^* = 12^7 \mod 55$

$= ((12)^2)^2 \times 12^2 \times 12 = 12^{4+2+1} \mod 55$.

$= (144)^2 \times 144 \times 12 =$

ahora $144 \equiv 34 \mod 55$

$= (34)^2 \times 34 \times 12 = \underbrace{1156}_{1} \times 34 \times 12 = \underbrace{34 \times 12}_{408} = \boxed{23}$

$1156 \equiv 1 \mod 55$

$408 \equiv 23 \mod 55$

ii) $e = 7$, $N = 5 \times 11$, $\varphi(N) = 40$, $d \equiv e^{-1} \bmod 40$

$1 = mcd(7,40) = mcd(7,5) = mcd(5,2) = mcd(2,1)$

$40 = 7 \times 5 + 5 \Rightarrow 5 = 40 - 7 \times 5$

$7 = 5 \times 1 + 2 \Rightarrow 2 = 7 - 5 \times 1$

$5 = 2 \times 2 + 1 \Rightarrow 1 = 5 - 2 \times 2$

$2 = 2 \times 1 + 0$

$1 = 5 - 2(7 - 5)$

$= 3 \times 5 + (-2)7$

$1 = 3 \times (40 - 7 \times 5) + (-2)7$

$\boxed{1 = 3 \times 40 - 17 \times 7}$

$-17 \equiv d \bmod 40$

$d = 23$

$C = 37$, solución $37^{23} \bmod 55 = 53$

↳ ¡parad aquí!

4] Esto, si has entendido los ejercicios anteriores, es fácil de responder, con $\varphi(N)$ el adversario puede calular e^{-1}, por tanto, SIEMPRE puede desifrar los mensajes que se envíen usando N como módulo... pero ¡hay más!

Veamos como un adversario puede, de hecho, encontrar los primos p y q tales que

$$N = pq$$

Sabemos que

$$\varphi(N) = (p-1)(q-1)$$

$$N = p \cdot q$$

Escribimos en rojo lo que el adversario conoce ya:

$$\varphi(N) = (p-1)(q-1) = pq - q - p + 1$$

$$N = p \cdot q$$

Esto es un sistema (¡no lineal!) de dos ecuaciones con dos incógnitas. Despejamos q en la primera

$$q = N - \varphi(N) + 1 - p$$

sustituimos en la segunda

$$N = p\,(N - \varphi(N) + 1 - p)$$

de donde tenemos

$$p^2 - (N - \varphi(N) + 1)p + N = 0$$

que es una ecuación de segundo grado con valor desconocido $\boxed{p}$. ¿Sabéis resolver ecuaciones de segundo grado? ...

☺ Pues eso, ¡el adversario también!

Si conoce $\varphi(N)$ ¡factorizará N! ¡Conoce todo!

5]

a)

d_1	d_2	
Bob	Beto	N módulo común
↑	↑	
e_1	e_2	

Si Bob conoce d_1, resulta que $d_1 e_1 \equiv 1 \mod \varphi(N)$, luego hace $d_1 e_1 - 1$ y sabe que eso es un múltiplo de $\varphi(N)$.

Como N es público, a partir de saber que

$\varphi(N) < N$

$d_1 e_1 - 1$ es múltiplo de $\varphi(N)$

acabará encontrando $\varphi(N)$. luego (¡remonda el ejercicio anterior!) sabrá todo.

Un ejemplo (pequeñito), $N = 11 \times 23 = 253$

$e_1 = 3$, $d_1 = 147$

Bob hace $d_1 \cdot e_1 - 1 = 440$

Sabe que $\exists \alpha \in \mathbb{Q}$

$\alpha \cdot \varphi(N) = 440$

$\varphi(N) < 253$

$440 = 2 \times 2 \times 2 \times 5 \times 11$

Candidatos a $\varphi(N)$ → 2 → 5 → 11

→ 2×2 → 5×2 → 11×2

→ $2 \times 2 \times 5$ → 5×11 → $5 \times 11 \times 2$

. . . . . (etc.)

¡buf! ¡¡muchos!!

¡Ojo! Como $\varphi(N) = \underbrace{(p-1)}_{\text{par}}\underbrace{(q-1)}_{\text{par}}$. $\varphi(N)$ es múltiplo de 4, eso reduce nuestra lista a:

4

$4 \times 2 = 8$

$20 = 4 \times 5$; $5 \times 11 = 55$

$4 \times 2 \times 5 = 40$

$4 \times 2 \times 11 = 88$

$4 \times 5 \times 11 = 220$

el que más "se parece" a N es 220, ¿probamos?

Sabemos que $\varphi(N) = N - p - q + 1$ luego...

$220 = 253 - (p+q) + 1 \Rightarrow p+q$ será 34;

¿Hay dos primos que sumen 34? ¡Sí! ¡11 y 23!

Además... ¡¡ $11 \times 23 = 253$!! (Ü) ¡Humaaa!

6] $m \xrightarrow{E} \left(f(r),\ m \cdot f(r),\ H(r)\right)$

¿Seguro?

No mucho... por ejemplo es MALEABLE. Si un adversario enuentia $c = (a, b, d)$ en el canal, sabe que, para un mensaje m y un valor aleatorio r (que él desconoce) se cumple

$$b = m \cdot f(r)$$

Así, eligiendo un mensaje $\bar{m}$ que le guste, puede construir $c^* = (a,\ \bar{m} \cdot b,\ d)$

que el receptor descifrará obteniendo $\bar{m} \cdot m$.

5 b) Bob e_1 N Berto e_2

Sabemos, por la Id de Bezout, que $\exists \alpha, \beta \in \mathbb{Z}$ tales que

$$\alpha e_1 + \beta e_2 = mcd(e_1, e_2) = 1$$

Como e_1 y e_2 son públicos, el adversario puede calcular α y β.

Dados dos cifrados C_1 y C_2 del mismo mensaje,

$$C_1 = M^{e_1} \mod N \longrightarrow \text{Bob}$$

$$C_2 = M^{e_2} \mod N \longrightarrow \text{Berto}$$

El adversario rompería M haciendo

$$M = C_1^{\alpha} \cdot C_2^{\beta} = M^{\alpha e_1 + \beta e_2} = M^1$$

Veamos un ejemplo con números, $M = 12$

$N = 55$, $e_1 = 7$, $e_2 = 5$

El adversario captura en el canal

$$C_1 = 12^7 = 23 \mod 55$$

y $$C_2 = 12^5 = 12 \mod 55$$

Calcula α y β:

$7 = 5 \times 1 + 2 \rightarrow 2 = 7 + (-1)5$

$5 = 2 \times 2 + 1 \rightarrow 1 = 5 - 2 \times 2$

$\Downarrow$

$1 = 3 \times 5 + (-2)7$

$\Rightarrow \alpha = -2, \beta = 3$

Así, calcula $M = 23^{-2} \cdot 12^3 = 23^{-2} \cdot 23 = 23^{-1} = \boxed{12}$ ← todo módulo 55

Universidad Rey Juan Carlos

Grado en Ingeniería de la Ciberseguridad

Criptografía

Ejercicios prácticas autodirigidas. Bloque 3. Cifrado Asimétrico.

---

1. Considera el siguiente esquema de intercambio de claves *a la* Diffie-Hellman, pero con matrices. Alice elige una matriz A (con elementos sobre, por ejemplo $\mathbb{Z}_p^*$, para p un primo grande) y calcula una inversa generalizada de A, que llamaremos A^g (es decir, A^g cumple que $AA^gA = A$) y envía a Bob A^gA. Bob elige una matriz B (también con entradas en $\mathbb{Z}_p^*$) calcula una inversa generalizada de B, B^g y envía a Alice A^gAB y A^gABB^g. Finalmente, Alice envía a Bob ABB^g. Ambos pueden así calcular la clave secrete, AB ,

   - Comprueba que el esquema anterior es correcto
   - Supón que alguna de las matrices que se envían en el canal es invertible. Analiza la seguridad del esquema (frente a un adversario pasivo).

2. Si elegimos un módulo RSA $N = 3337$, da opciones adecuadas e, d para completar la generación de claves.

3. Considera una modificación del esquema de cifrado de Bellare y Rogaway en la que el cifrado de un texto m conste de tres componentes:

   - $F(r)$, con r aleatorio y F una función *one-way*,
   - $m \cdot F(r)$,
   - $H(m)$, con H un oráculo aleatorio

   Analiza informalmente la seguridad del esquema resultante.

4. Considera un esquema de cifrado de clave pública en el que el cifrado de un texto m conste se construya como $(f(r), H(m) \oplus r)$, donde f es una función de una vía (que transforma cadenas de bits en cadenas de bits del mismo tamaño, ℓ), H es una función hash (con rango en $\{0,1\}^\ell$) y r es una cadena aleatoria de ℓ bits que se genera *fresca* cada vez que invocamos al algoritmo de cifrado. Analiza informalmente esta construcción.

5. Vamos ahora a considerar un esquema de cifrado que utiliza polinomios (cuyos coeficientes estarían en un cuerpo finito). Supongamos que la clave pública es un polinomio de grado n, $p(x) = a_0 + a_1x + a_2x^2 + \cdots$. La clave secreta es una raíz r de p, es decir, $p(r) = 0$. El parámetro de seguridad fija el tamaño de los coeficientes y el grado del polinomio (por ejemplo, si ℓ es el parámetro de seguridad trabajamos en un cuerpo de "más o menos"ℓ elementos y p tiene grado polinomial en ℓ). El cifrado de un mensaje m se construye eligiendo un polinomio q al azar (con coeficientes aleatorios en el cuerpo finito dado), y de grado n, y luego construyendo el cifrado como

   $$c := p(x)q(x) + m.$$

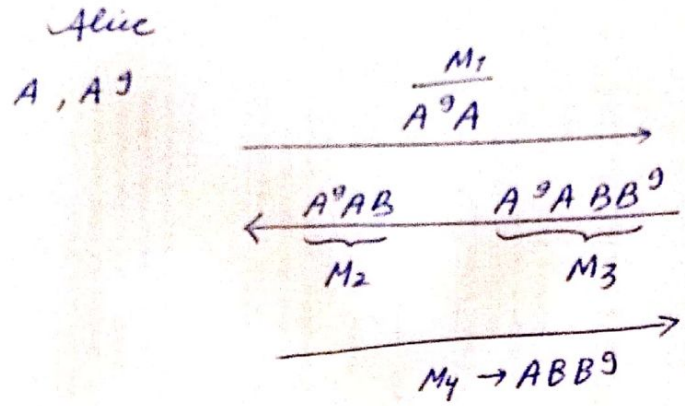
   Describe cómo se realizaría el descifrado. Analiza la seguridad de esta construcción contestando, al menos, las siguientes preguntas:

   a. ¿Qué es necesario pedir en la elección de las claves, para que pueda haber seguridad de tipo *one-way*?

   b. ¿El diseño actual, con algún tipo de generación de claves, puede ser IND-CCA2?

CRIPTOGRAFÍA. HOJA 3. PRÁCTICAS AUTODIRIGIDAS

1]



Llamamos M_i, $i=1,..,4$ a los mensajes insertados en el canal (ver dibujo), es decir:

$M_1 = A^9A$, $M_2 = A^9AB$, $M_3 = A^9ABB^9$ y $M_4 = ABB^9$

Recordamos que $AA^9A = B$ y $BB^9B = B$

a) Conexión: Veamos que los mensajes descritos pueden construirse, y que tanto Alice como Bob pueden obtener la clave común $K = A \cdot B$.

Alice: . Construye M_1 sin problema, y M_4 como

$$AM_3 = AA^9ABB^9 = ABB^9$$

. Construye K haciendo

$$K = A \cdot M_2$$

Bob: . Construye $M_2 = M_1 B$ y $M_3 = M_2 B^9$

. Construye $K = M_4 B$.

b) Seguridad: Un adversario pasivo observa el CANAL, sabe calcular K si conoce, por ejemplo

$\boxed{M_1^{-1}}$ (pues $M_1^{-1} \cdot M_2 = B$, y $K = M_4 B$)

2| RSA con $N = 3337$. i e. d?

Primero: necesito factorizar N, como producto de dos primos p y q

Luego: busco e, d tales que

$$ed \equiv 1 \mod \phi(N)$$

con $\phi(N) = (p-1)(q-1)$

! Todo número no primo tiene algún divisor primo menor que su raíz.

Así, probaremos para buscar p y q los números desde 1 al 57 (pues $\sqrt{3337} \simeq 57$)

Ahora, descartamos 1, 2, 3, 5 fácilmente

; podemos mirar desde el final: los primos más grandes cercanos a 57 son 53, 47 y 43

¡pensad!
$50^2 = 2500$
$60^2 = 3600$
a ojo sabíamos que mayor que 60 no es!

y resulta que $3337 \mid 47$, 0, 71

y 71 también es primo!

Así, $N = 71 \cdot 47$. $\phi(N) = 70 \times 46 = 3220$

2 | (cont.)

Busco e, d con $ed \equiv 1 \mod 3220$

Si cojo e con $\text{mcd}(e, 3220) = 1$ sé que existe d (en otro caso e no tiene inverso módulo 3220).

Ahora

3220	2
1610	2
805	5
161	7
23	23
1	

$3220 = 2^2 \cdot 5 \times 7 \times 23$

luego puedo coger $e = 3$, que no tiene ningún divisor común con $\varphi(N) = 3220$. Ahora, calculo d^{-1} usando el algoritmo de Euclides

$\text{mcd}(3220, 3) = \text{mcd}(3, 1) = 1$

$3220 = 1073 \times 3 + 1 \Rightarrow 1 = 3220 + (-3)\,1073$

$= 3220 + 3 \times (-1073)$

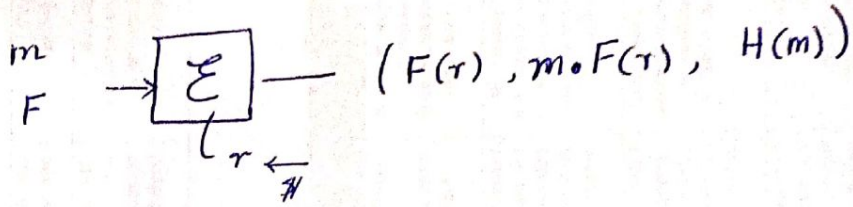
↑ esto es el "d" de la Id. de Bezout

Basta tomar $d \equiv -1073 \mod 3220$, por ejemplo $\boxed{d = 2.147}$

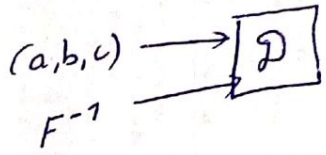
3] Bellare & Rogaway modificado (otra vez)

F ; función de una vía [$pk = F$, $sk = F^{-1}$]

H ; oráculo aleatorio (hash ideal)



¿Cómo se descifraría?



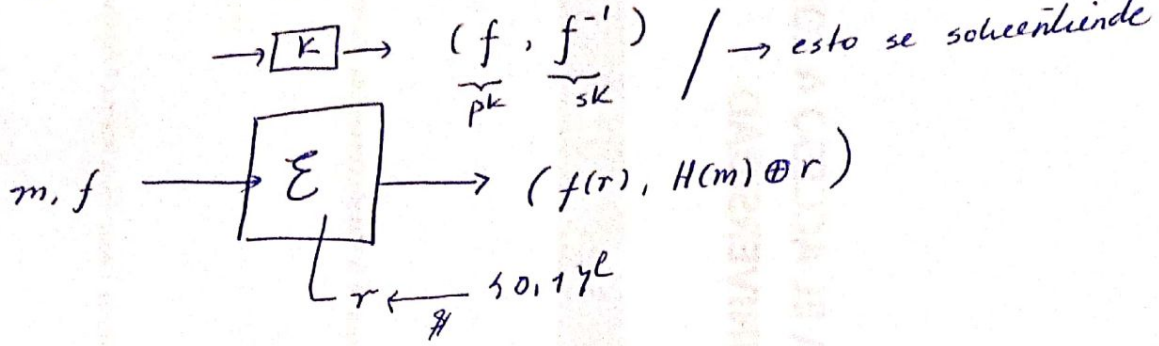
1. $r = F^{-1}(a)$
2. $m = \frac{b}{F(r)}$
3. Check $H(m) = c$
   if $\neq$, output $\perp$
   else, output m

¡Ataque! el paso 2. puede hacerlo cualquiera ; $\boxed{m = b/a}$

Si es posible dividir en la estructura algebraica subyacente (¡que lo ha de ser, para que se pueda descifrar!), este esquema es inseguro (no es siquiera OW-CPA).

4] $f: \{0,1\}^\ell \longrightarrow \{0,1\}^\ell$ es de UNA VÍA

$H: \{0,1\}^* \longrightarrow \{0,1\}^\ell$ es un hash



No es un esquema conecto pues H no es reversible, es decir, ¡no es posible descifrar!

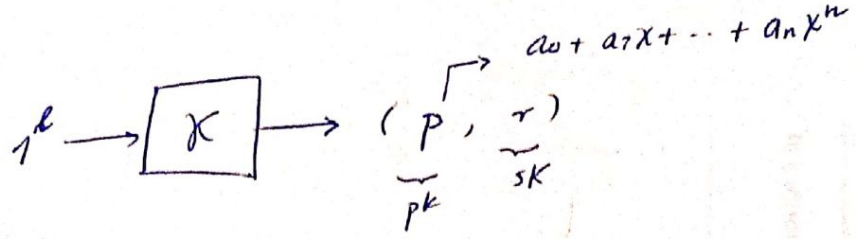
Con f^{-1} (la clave secreta) dado un texto cifrado (a,b), hacemos

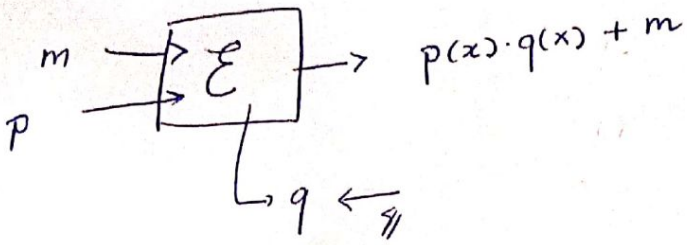
- $r = f^{-1}(a)$
- $H(m) = r \oplus b$

pero sólo obtenemos $H(m)$!!

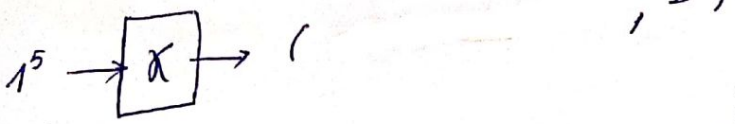
No miramos seguridad, pues el esquema ni siquiera es conecto...

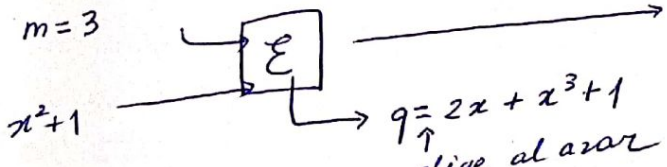
5/





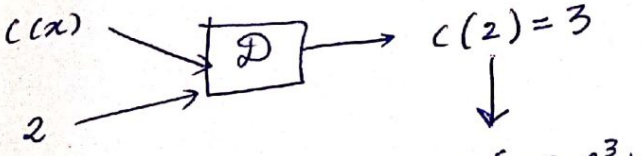
Un ejemplo con números, trabajamos en $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$





¡fíjate! los textos cifrados son polinomios

$$C(x) = (x^2+1)(2x + x^3 + 1) + 3$$
$$= x^5 + 3x^3 + x^2 + 2x + 4$$



$$2^5 + 3\cdot 2^3 + 2^2 + 2\cdot 2 + 4 \mod 5$$
$$\| \quad 68$$

Para descifrar, como $C(x) = p(x)\cdot q(x) + m$, evaluamos ese polinomio en $x = r$, y como $p(r) = 0$, se tiene

$$C(r) = 0 \cdot q(r) + m = m.$$

Vamos ahora con la seguridad...

a) La seguridad OW se obtiene si, viendo un texto cifrado $c(x)$ no obtenemos información acerca del mensaje que x cifra. ¿Cómo podemos evitar estos ataques al generar las claves?

$pk \rightarrow p(x)$

$r \in$ cuerpo que usamos, $/\ p(r) = 0$.

Es, por tanto, <u>fundamental</u>, que no sea fácil factorizar p, es decir encontrar sus raíces. Si tomamos los valores del ejemplo anterior (super-pequeño y super-inseguro!) el adversario puede fácilmente probar con todos los valores de $\mathbb{Z}_5$ a la caza de la clave secreta:

x	x^2+1
0	1
1	2
2	0
3	0
4	2

> tanto $r=2$ como $r=3$ le sirven para descifrar!!

b) **IND-CCA2**

¡Nunca! Por el hecho de que es <u>maleable</u>. Dado un cifrado $c(x)$, $c(x) + \tilde{m}$ es un cifrado de $\tilde{m}+m$

Universidad Rey Juan Carlos

Grado en Ingeniería de la Ciberseguridad

Criptografía

Ejercicios prácticas autodirigidas. Bloque 4. Firmas y Protocolos.

---

1. Demuestra que el esquema de compartición de secretos de Shamir es lineal, es decir, si disponemos de dos shares s_1 y s_2 para dos secretos S_1 y S_2 (resp.) podemos construir a partir de s_1, s_2 una share para el secreto $S_1 + S_2$ y del mismo modo, dada una share para un secreto S y un escalar λ en el cuerpo en el que trabajamos, podemos construír una nueva share para el secreto λS.

2. Supongamos que $\mathcal{E} = (G, E, D)$ es un esquema de cifrado de clave pública seguro IND-CPA. Constuye a partir de $\mathcal{E}$ un esquema de compromiso.

3. Definimos un esquema de compromiso a partir de un esquema

$$\Pi = (KeyGen, Enc, Dec)$$

de cifrado de clave pública, correcto y determinista (que cifra siempre cada mensaje de la misma manera, sin involucrar aleatoriedad), haciendo:

   - Setup; con entrada el parámetro de seguridad λ, ejecuta $KeyGen(1^\lambda)$ y da como salida la clave pública pk que éste devuelve;
   - Commit; con entrada un mensaje m y la clave pública pk, llama $Enc(pk, m)$ y da como output su salida, el cifrado c
   - Open; con entrada c, pk da como salida m (si se cumple $c = Enc(pk, m)$) y $\perp$ en otro caso.

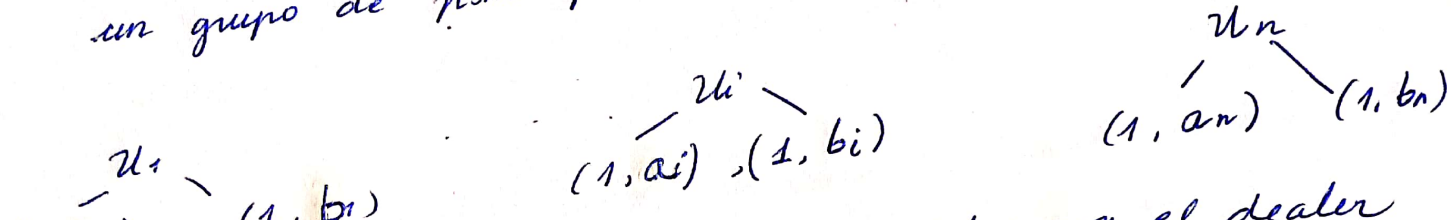
   Comenta si se cumplen las dos propiedades esenciales de este tipo de esquemas.

4. Supongamos que existe un esquema de firma digital con la propiedad de que dos usuarios distintos U_1 y U_2 son capaces de generar con sus claves secretas dos firmas idénticas σ de modo que, para todo mensaje m (que suponemos es un elemento de un cierto $\mathbb{Z}_p$ se tiene que (m, σ) es validado con la clave pública de verificación de U_1 y (m^2, σ) es validado con la clave pública de verificación de U_2. ¿Es este esquema seguro?

Soluciones - Alumnos (4)

1. Shamir es LINEAL.

Dados dos secretos, S_1 y S_2, supongamos que un dealer "D" ha repartido shares del esquema de Shamir en un grupo de participantes $u_1, \dots, u_n$.



siendo f y g polinomios construidos por el dealer con

$$f(0) = S_1 \qquad g(0) = S_2$$
$$f(1) = a_1 \qquad g(1) = b_1$$
$$f(2) = a_2$$
$$\vdots \qquad \vdots$$
$$f(n) = a_n \qquad g(n) = b_n$$

ahora bien, claramente, si el esquema original tiene umbral t (f y g son de grado $t-1$), tenemos que:

$$f(x) = \underbrace{f_0}_{S_1} + f_1 x + \dots + f_{t-1} x^{t-1}$$

$$g(x) = \underbrace{g_0}_{S_2} + g_1 x + \dots + g_{t-1} x^{t-1}$$

y

$$(f+g)(x) = \underbrace{f_0 + g_0}_{S_1 + S_2} + (f_1 + g_1)x + \dots + (f_{t-1} + g_{t-1}) x^{t-1}$$

Es decir: el polinomio suma tiene como término independiente $s_1 + s_2$ y es de grado $t-1$.

Si los usuarios "suman" sus shares:

u_1 ... u_n

$(1, a_1+b_1)$ ... $(1, a_n+b_n)$

está claro que t de ellos reconstruyen el polinomio $f+g$, y por tanto el "nuevo secreto", s_1+s_2.

Para el producto escalar razonamos igual: cada usuario tiene $u_i \leftrightarrow (i, h(i))$ con

$$h(X) = \underbrace{h_0}_{s} + h_1 X + \dots + h_{t-1} X^{t-1},$$

multiplica por λ su "share" y $u_i \to (i, \underline{\lambda h(i)})$

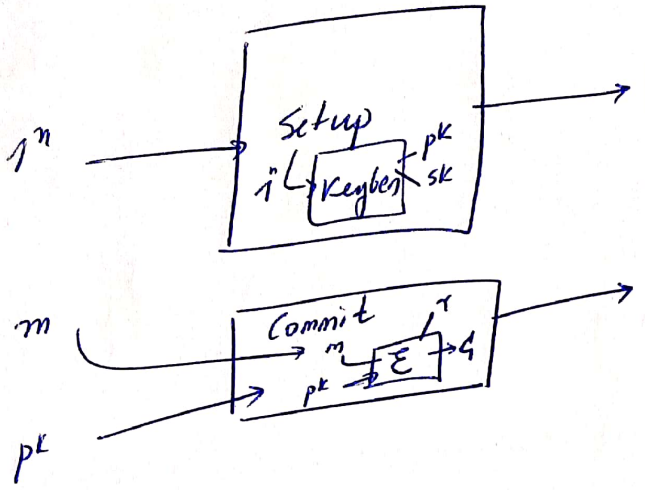
Ahora, t usuarios pueden, juntando sus shares, reconstruir el polinomio $\lambda h(X) = \lambda s + \lambda h_1 X + \dots + \lambda h_{t-1} X^{t-1}$

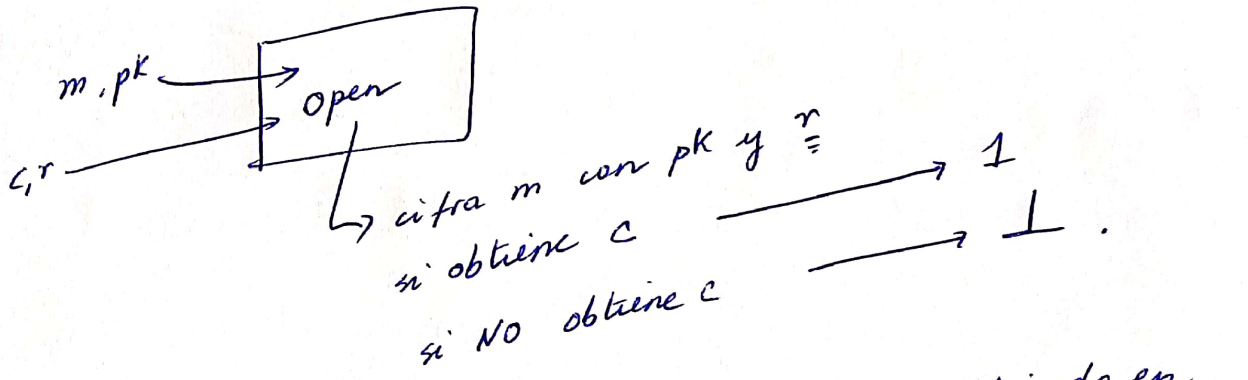
y obtener λs. ⌐

2] Vamos a construir un esquema de compromiso

$\mathcal{C} = (Setup, Commit, Open)$

partiendo de nuestros algoritmos $(Keygen, E, D)$ del esquema de cifrado IND-CPA.



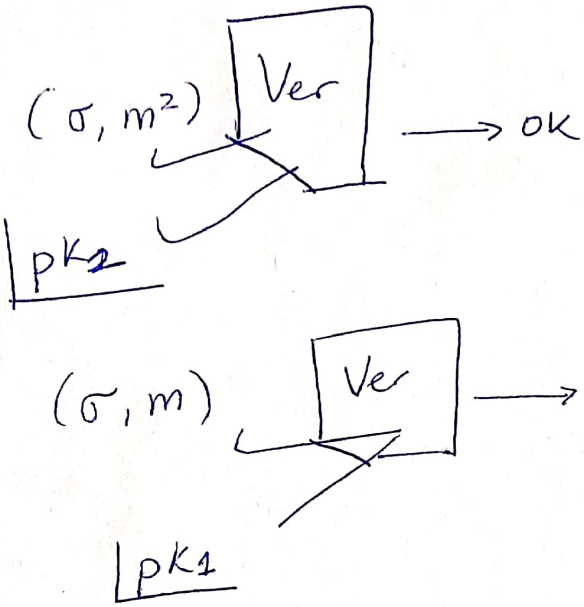


3] La idea sigue el espíritu de nuestra solución explicada en (2) pero como el esquema es DETERMINISTA, el compromiso no es HIDING: el cifrado "c" filtra información sobre m, pues $\mathcal{C}$ no es IND-CAA (al ser determinista)

4

u_1 , u_2

$\hookrightarrow \sigma$ $\hookrightarrow \sigma$



Claramente NO es seguro, pues u_1 puede generar (σ, m^2) que será validado con pk_2, i.e. ¡sin que u_2 sepa nada del mensaje!

Universidad Rey Juan Carlos

Grado en Ingeniería de la Ciberseguridad

Criptografía

Sesión 5. Clave Pública (II).

---

1. Considera una generación RSA de claves anómala donde

   a) N es un número primo

   b) N es producto de tres números primos, p, q, r.

   Comenta qué problemas de seguridad o ventajas puede tener la generación en el caso a), y estudia la corrección del esquema resultante con la generación b).

2. Considera el cifrado de Rabin (RSA con exponente de cifrado igual a 2). Si el módulo público es N, supón que conoces un valor $\epsilon \neq -1, 1$ tal que $\epsilon^2 = 1 \bmod N$. Analiza la seguridad del esquema en el sentido:

   - a) NM-CPA
   - b) IND-CCA2
   - b) IND-CPA
   - c) OW-CPA

3. Vamos ahora a considerar un esquema de cifrado que utiliza polinomios (cuyos coeficientes estarían en un cuerpo finito). Supongamos que la clave pública es una pareja de polinomios del mismo grado n,

   $$p(x) = a_0 + a_1 x + a_2 x^2 + \cdots, + a_n x^n \text{ y } q(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_n x^n.$$

   La clave secreta es una raíz r de p, es decir, $p(r) = 0$. Para cifrar mensajes, contemplamos las siguientes opciones:

   a) $c = p(x)q(x) + m$

   b) $p(x)q(x) + q(x) + m$

   c) $t(p(x)q(x)) + m$, con t elegido uniformemente al azar.

   Describe en cada caso como se realizaría el descifrado. Analiza la seguridad de esas opciones, al menos en el sentido IND-CPA, IND-CCA2, NM-CPA, NM-CCA2.

4. Un esquema de Zeng-Seberry. Sea G un grupo de orden primo q generado por un elemento g. Supongamos que V es una función que coge un elemento h del grupo y construye $V(h)$, una cadena de bits *aleatoria*. Considera H una función hash. La clave pública del esquema será G, g, y donde $y = g^x$ y $x \in \{1, \ldots, q-1\}$ es la clave secreta. Para cifrar un mensaje m se siguen los siguientes pasos:

   a) Se elige $k \in \{0, ..., q-1\}$ al azar

   b) se define $z := V(y^k)$

   c) se define $t := H(m)$

   d) se construye el texto cifrado $c = (c_1, c_1) = (g^k, z \oplus (m \| t))$

   Piensa en los rangos y dominios de V y H para que la descripción anterior sea correcta. Describe el algoritmo de descifrado. Analiza la seguridad CCA2 del esquema anterior.

[Criptografía - Ing. ciberseguridad
Sesión 5. Clase Magistral [grupos separados]]

1] Generación RSA anómala

a) Si N es primo, $\varphi(N)$ es simplemente $N-1$.
Con $\varphi(N)$ es fácil para un adversario calcular toda clave secreta d asociada a ese módulo N

b) $N = P \cdot q \cdot r$
Entonces, si esos primos son distintos, $\varphi(N) = (p-1)(q-1)(r-1)$
y podríamos generar claves e y d con
$\text{mcd}(e, \varphi(N)) = \text{mcd}(d, \varphi(N)) = 1$ y $ed \equiv 1 \bmod \varphi(N)$.
Así, si cogemos $m \in \mathbb{Z}_N$ (y $\text{mcd}(m, N) = 1$)

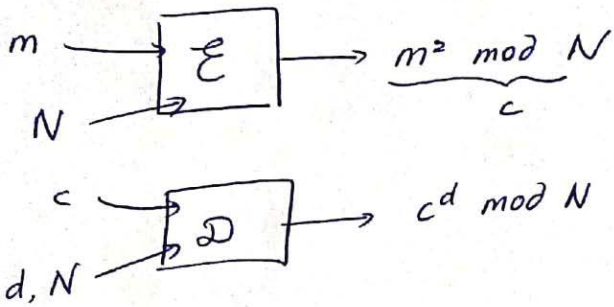
$$m^{ed} \equiv m \bmod N$$

luego TODO funcionaría bien. El esquema puede así hacerse correcto.

2] Cifrado Rabin

Es RSA con $e=2$ (fijo), es decir

$de \equiv 1 \bmod \varphi(N)$
$N = P \cdot q$, P y q primos elegidos al azar con $\log_2 P \sim \log_2 q \sim K$



a) **NM-CPA** No

Igual que RSA, Rabin es maleable. Si $\mathcal{A}$ obtiene como objetivo c^* sigue esta estrategia:

1. Elige $\tilde{m} \in \mathbb{Z}_N^*$
2. Construye $\bar{c} = (\tilde{m})^2 c^* \bmod N$
3. Da al simulador $\mathcal{S} \rightarrow (\bar{c}, R)$

con $R(a,b) = 1$ si $a = \tilde{m} b$

(claramente $R(\bar{c}, c^*) = 1$, pues $\bar{m} = \tilde{m} \cdot m^*$)

b) **IND-CCA2** No

$\mathcal{A}$ no ser (por a)) NM-CPA, no es NM-CCA2, que es equivalente a IND-CCA2, luego no es IND-CCA2.

c) **IND-CPA** No

Es <u>determinista</u> luego en el juego IND el adversario gana siempre, pues elige m_0, m_1, calcula $m_0^2 \bmod N$ y $m_1^2 \bmod N$ y compara con el reto c_b^* para decidir qué ha usado el simulador.

d) **OW-CPA**

No lo es, si el adversario A conoce un ε como el del enunciado. La razón es la siguiente:

si $\varepsilon^2 = 1 \bmod N$ $\quad (\varepsilon+1)(\varepsilon-1)$ es múltiplo de N

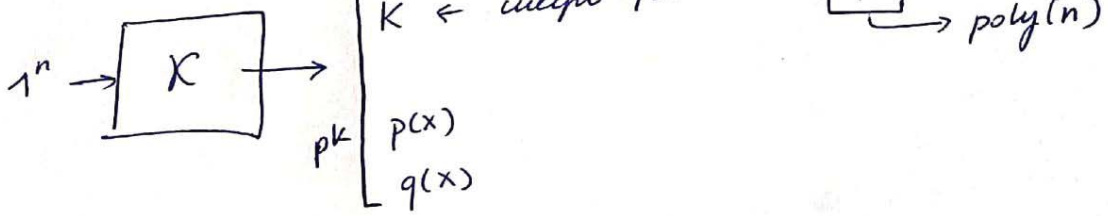
si $\varepsilon - 1 < N$ (por ejemplo),

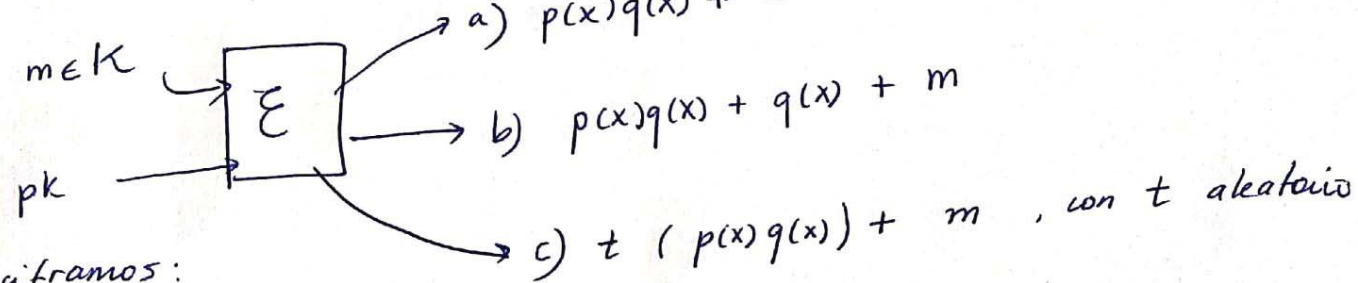
$\gcd((\varepsilon-1), N)$ es, p o q. luego conoce ε

lleva a factorizar $N \Rightarrow$ ¡lleva a descifrar lo que queramos!

> Este ejercicio es algo avanzado, me basta con que recordéis que es OW-CPA $\iff$ factorizar N es OW, ¡igual que RSA de libro de texto!

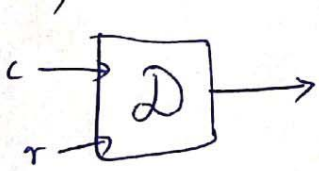
3/



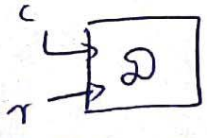


Desciframos:

a)

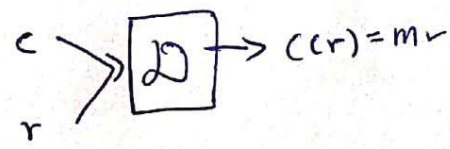


b)



$c(r) - q(r) = m$ ✓

c)



Análisis de seguridad

a) y b) son cifrados DETERMINISTAS, nunca serán IND.

a) y b) son maleables por un adversario CPA, pues

$c^* + \tilde{m}$ es un cifrado de $m^* + m^*$

luego no son NM-CPA (y no son, por tanto, NM-CCA2).

ya lo sabíamos al no ser IND-CCA2

c) ¿IND-CPA?

c^* reto;

$c_0 = t(p(x)\,q(x)) + m_0$

$= \underbrace{\quad\quad}_{\text{términos del polinomio con } x, x^2 \ldots} + \underbrace{taobo + m_0}_{\text{término independiente}}$.

$c_1 = \underbrace{\quad\quad}_{} + \underbrace{\bar{t}aobo + m_1}$

Cada vez que se cifra un mensaje se le suma un MULTIPLO ALEATORIO de aobo, luego se hace una especie de ONE TIME PAD. (Vernam cipher) $\Rightarrow$ Es **IND-CPA**

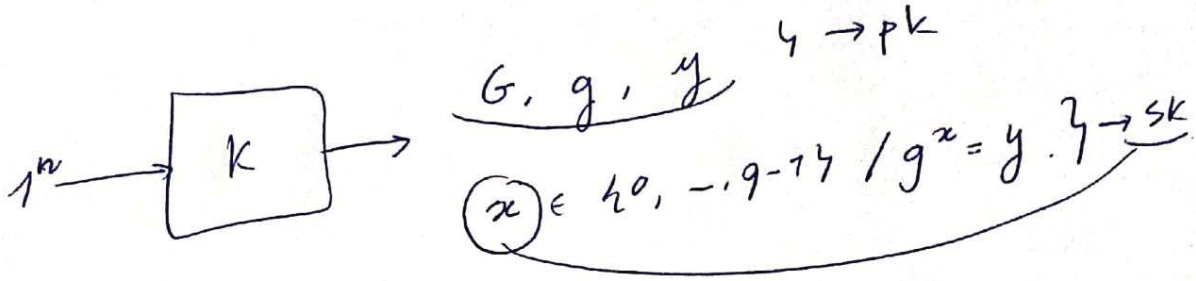
4] [Zheng - Seberry]

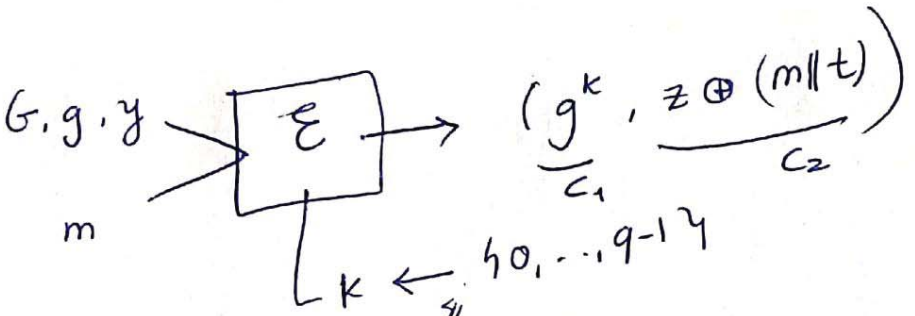
$G = \{g^0, g, g^2, \ldots, g^{p-1}\}$ g ; q primo

$\|$
1_G

$V: G \longrightarrow \{0,1\}^*$

H hash





$t := H(m)$

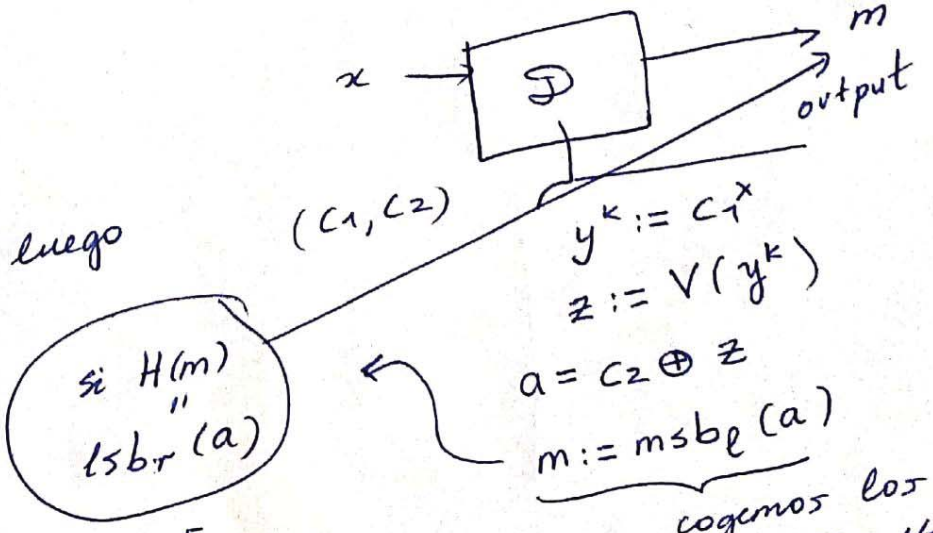
$z := V(y^k)$

- $V(y^k)$ tiene que ser de la misma longitud que $m \| t$ si ciframos mensajes de ℓ bits, y $H: \{0,1\}^* \longrightarrow \{0,1\}^r$

$V: G \longrightarrow \{0,1\}^{r+\ell}$

- Descifrado:

$c_1^x = y^k$ luego



Es decir:

. Calcula y^k

. Calcula z

. Recupera a (debería ser $m \| t$)

. Comprueba que

$H(m)$ = r últimos bits de a.
$\uparrow$
ℓ bits más altos de a.

. Si todo OK, da m como salida.

Seguridad CCA2.

$$c^* = \left(g^{(k)} \leftarrow \text{al azar} \; ; \; V(y^k) \oplus (m_b \| H(m_b)) \right)$$

c_1^* $\qquad$ c_2^*

es un texto objetivo cualquiera, sé cómo se estructura

Ataque CCA2. sé que c^* es un cifrado de m_0 ó m_1

construyo, para un $\bar{m} \neq m_0, \bar{m} \neq m_1$ el cifrado

$$c_A = \left(c_1^*, c_2^* \oplus (m_1 \| H(m_1)) \oplus (\bar{m} \| H(\bar{m})) \right)$$

Si c^* es un cifrado de m_1,

$$c_2^* \oplus m_1 \| H(m_1) = V(y^k)$$

luego $$c_A = \left(\underbrace{g^k}_{c_1^*} \; ; \; V(y^k) \oplus (\bar{m} \| H(\bar{m})) \right)$$

A usa su oráculo CCA_2:

Así, si c^* cifraba m_1

$$c_A \longrightarrow O_D \longrightarrow \bar{m}$$

si c^* cifraba m_0

$$c_1 \longrightarrow O_D \longrightarrow \perp$$

¡y eso ayuda al adversario a distinguir!

No es IND-CCA2

Universidad Rey Juan Carlos

Grado en Ingeniería de la Ciberseguridad

Criptografía

Sesión 6. Firma digital. Protocolos criptográficos.

---

1. Jugando a piedra, papel o tijera. Supongamos que Alice y Bob quieren jugar a piedra, papel o tijera a través de un sistema de mensajería, y lo hacen usando una función hash H – definida en el dominio apropiado – siguiendo el siguiente protocolo:

   Paso 1. Alice elige $s_A \in \{\texttt{piedra}, \texttt{papel}, \texttt{tijera}\}$. Elige una cadena de bits al azar r_a y envía a Bob el resumen $h_A = H(r_a || s_a)$

   Paso 2. Bob elige $s_B \in \{\texttt{piedra}, \texttt{papel}, \texttt{tijera}\}$ y se lo envía a Alice,

   Paso 3. Alice envía a Bob r_a, s_a. Ahora, Bob comprueba que el hash de los valores recibidos coincide con h_A y, si es correcto, ambos aceptan el resultado del juego.

   ¿Con qué tipo de protocolo criptográfico asocias esta construcción? ¿qué propiedad de este protocolo garantizaría que es justo para Alice? ¿Y para Bob? ¿qué hemos de pedir a la función hash H para que esas propiedades se cumplan?

2. Trabajaremos en $\mathbb{Z}_{17}^*$ y vamos a compartir un secreto $S = 2$ usando un esquema de Shamir con umbral 3, es decir, para que se requiera un mínimo de 3 "shares"de la forma $s_i = (i, f(i))$ de cara a recuperar el secreto. Recordemos que éste se calcula obteniendo un poninomio f, que en este caso será de grado 2, cuyo término independiente es el secreto.

   Escribe los valores que recibirá un conjunto de $n = 6$ participantes, estudia cómo recuperan el secreto los participantes del conjunto $\{P_1, P_2, P_3\}$ y justifica que un conjunto (cualquiera, de tu elección) de dos participantes no aprende nada sobre S.

3. Una firma de Lamport es una esquema de firma seguro para un sólo uso que se puede construir a partir de una función $f : X \to Y$ de una vía. A continuación describimos la generación de claves y el algortimo de firma del esquema de firma de Lamport para firmar un mensaje m consistente en una cadena de v bits, es decir, $m \in \{0,1\}^v$.

   Generación de claves: Para cada $i \in \{0,1\}$ y para cada $j \in \{1, 2, 3, \ldots, v\}$ se genera uniformemente al azar un valor $x_{i,j} \in X$ y se calcula $y_{i,j} = f(x_{i,j}) \in Y$. Se obtienen $2v$ valores en X, que constituyen la clave secreta, y otros $2v$ valores en Y, que constituyen la clave pública. Representados más visualmente, en forma de matriz, tenemos:

$$sk := \begin{pmatrix} x_{0,1} & x_{0,2} & x_{0,3} & \ldots & x_{0,v} \\ x_{1,1} & x_{1,2} & x_{1,3} & \ldots & x_{1,v} \end{pmatrix}$$

$$pk := \begin{pmatrix} y_{0,1} & y_{0,2} & y_{0,3} & \ldots & y_{0,v} \\ y_{1,1} & y_{1,2} & y_{1,3} & \ldots & y_{1,v} \end{pmatrix}$$

   Algoritmo de firma: Dado un mensaje $m = b_1 b_2 \ldots b_v \in \{0,1\}^v$ donde cada b_j es un bit. La firma de m se calcula eligiendo, para cada j, uno de los dos posibles valores $x_{i,j}$ dependiendo del valor del bit b_j, el de la fila superior si $b_j = 0$ y el de la fila inferior si $b_j = 1$. Más formalmente:

$$\sigma = (x_{b_1,1}, x_{b_2,2}, x_{b_3,3}, \ldots, x_{b_v,v}) \in X^v$$

   a) Trata de describir el algoritmo de verificación.

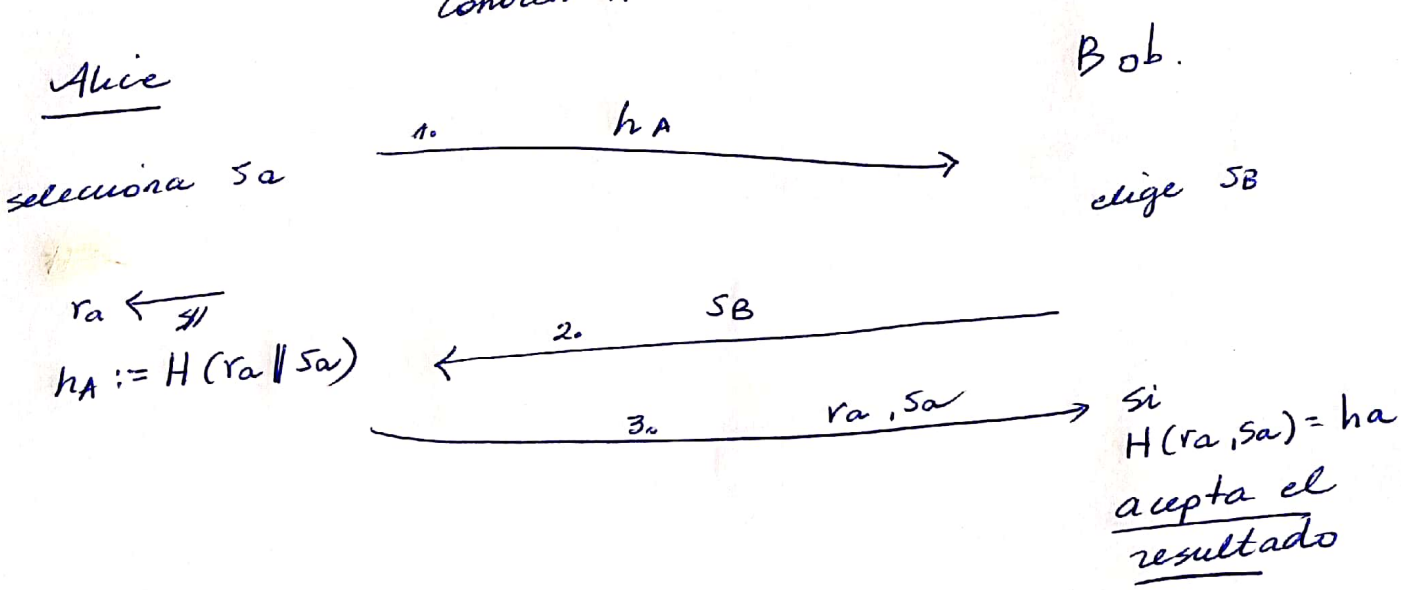
   b) Da una idea informal de por qué el esquema es seguro cuando se utiliza una única vez.

   c) Explica por qué el esquema es completamente inseguro cuando se utiliza varias veces.

Hoja Magistral 6. Firma digital. Protocolos.

1] Piedra, papel o tijera

Lo que Alice y Bob necesitan es un ESQUEMA DE COMPROMISO que consiga el hecho de que, usando una red, no se garantiza que ambos revelen su elección simultáneamente.



Justo para Alice: (hiding!)
Bob no debe conocer s_a antes de hacer su elección de s_B, por tanto h_A no debe revelar nada sobre el valor s_a.
(h_A se ha de computar como un random oracle)

Justo para Bob: (binding!)
Alice no debe ser capaz de, tras recibir s_B, cambiar su elección s_a original por otra más ventajosa.

Matemáticamente no debe ser posible para calcular $\tilde{r}_a$, $\tilde{s}_a$ con $\tilde{s}_a \neq s_a$ y

$$H(r_a \| s_a) = H(\tilde{r}_a \| \tilde{s}_a)$$

En particular esto puede garantizarse si H es CR (resistente a colisiones)

Así, necesitamos que H sea un random oracle (bueno, en realidad eso es una condición SUFICIENTE).

2 | Shamir sobre $\mathbb{Z}_{17}^*$ $\quad S = 2 \quad k = 3$;

Calculamos "al azar" f (polinomio de grado 2 sobre $\mathbb{Z}_{17}^*$)

$\mathbb{Z}_{17}^* = \{0, 1, \ldots, 16\}$

$f(x) = f_0 + f_1 x + f_2 x^{(2)}$ $\longrightarrow k-1$

$f_0 = 2 \qquad f_1 = 3 \qquad f_2 = 8$ (elegí al azar f_1 y f_2)

Voy a construir las "shares" para 6 usuarios

$u_1 \to (1, f(1)) \; ; \; f(1) = 2 + 3 \cdot 1 + 8 \cdot 1^2 = 13$

$u_2 \to (2, f(2)) \; ; \; f(2) = 2 + 3 \cdot 2 + 8 \cdot 2^2 = 6$

$u_3 \to (3, f(3)) \; ; \; f(3) = 2 + 3 \cdot 3 + 8 \cdot 3^2 = 15$

$u_4 \to (4, f(4)) \; ; \; f(4) = 2 + 3 \cdot 4 + 8 \cdot 4^2 = 6$

$u_5 \to (5, f(5)) \; ; \; f(5) = 2 + 3 \cdot 5 + 8 \cdot 5^2 = 13$

$u_6 \to (6, f(6)) \; ; \; f(6) = 2 + 3 \cdot 6 + 8 \cdot 6^2 = 2$

¡ojo, cuentas módulo 17!

- $\{u_1, u_2, u_3\}$ recuperan el secreto usando sus shares

$(1,13)$ $(2,6)$ y $(3,6)$
y_1 y_2 y_3

con la fórmula

$$f(0) = \sum_{i=1}^{3} y_i \prod_{j \neq i} \frac{-j}{i-j} \mod 17$$

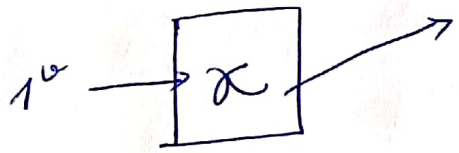
$$f(0) = y_1\left(\frac{-2}{1-2}\cdot\frac{-3}{1-3}\right) + y_2\left(\frac{-1}{2-1}\cdot\frac{-3}{2-3}\right) + y_3\left(\frac{-1}{3-1}\cdot\frac{-2}{3-2}\right)$$

$$= 13\times\left(\frac{6}{2}\right) + 6\times(-3) + 15\left(\frac{2}{2}\right) =$$

$$= 13\times 3 - 18 + 15 = 2 \quad \checkmark$$

[Era el secreto escondido!]

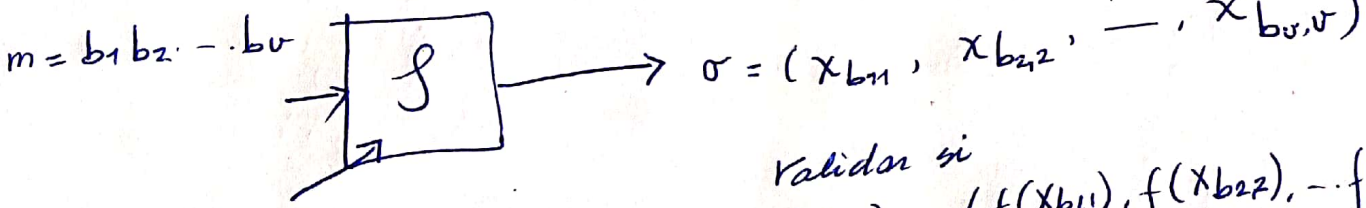
3] Firmas de Lamport



$$sk = \begin{pmatrix} x_{0,1} & x_{0,2} & \cdots & x_{0,v} \\ x_{1,1} & x_{1,2} & \cdots & x_{1,v} \end{pmatrix}$$

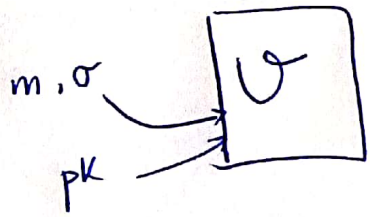
$\sum f$

$$pk = \begin{pmatrix} y_{0,1} & y_{0,2} & \cdots & y_{0,v} \\ y_{1,1} & y_{1,2} & & y_{1,v} \end{pmatrix}$$



sk

a)



validar si

$$f(\sigma) = (f(x_{b_{1,1}}), f(x_{b_{2,2}}), \ldots f(x_{b_{v,v}}))$$
$$\| $$
$$(y_{b_{1,1}}, y_{b_{2,2}}, \ldots, y_{b_{v,v}})$$

si $=$ $\longrightarrow$ ok ✓

else $\longrightarrow$ $\perp$. ¡no válida

b) Es seguro porque sin conocer sk (los x) no podemos construirlos a partir de pk sin invertir f.

Ejemplo: si $v=1$ (para mensajes de un bit)

si $sk = \begin{pmatrix} x_{0,1} \\ x_{1,1} \end{pmatrix}$

$m=0$ se firma con $\sigma = x_{0,1}$

$\overline{m}=1$ " " " $\overline{\sigma} = x_{1,1}$

Si quiero "falsificar" σ (no conozco $x_{0,1}$), tendré que calcularla a partir de $pk = \begin{pmatrix} y_{0,1} \\ y_{1,1} \end{pmatrix}$: luego eso es tan difícil como calcular $f^{-1}(y_{0,1})$ (que es muy difícil si f es de una vía.

este valor no es útil, no se relaciona con $x_{0,1}$.

c) Supongamos que dispongo de un par

(m, σ)

firmado con $sk = \begin{pmatrix} x_{01} & x_{12} & x_{0v} \\ x_{11} & x_{12} & x_{1v} \end{pmatrix}$

si $m = (b_1, \ldots, b_v)$ y

$\sigma = (x_{b_1,1}, \ldots, x_{b_v,v})$

conocer σ me da LA MITAD de la clave secreta!!