TEORÍA DE CÓDIGOS Y CRIPTOGRAFÍA

Curso 2024-25

Hoja nº 3

Criptografía Asimétrica

1. Ana y Beatriz cifran sus mensajes con el criptosistema de Cesar sobre el alfabeto castellano de 27 letras. Para poder cambiar de clave con frecuencia, deciden emplear el intercambio de claves de Diffie-Hellman. Para implementar el intercambio acuerdan que verán las 27 claves, $\{A, \dots, Z\}$ como las clases $\{1, \dots, 27\} \subset (\mathbb{Z}/29)^*$, y que utilizarán el logaritmo discreto en $\mathbb{F}_{29}^* = (\mathbb{Z}/29)^*$ con base $g = 2$.

a) Supón que Ana elige como exponente en el intercambio $a = 5$ y Beatriz $b = 8$. ¿Cómo cifrarán el mensaje *HOLA* con la clave resultante?

b) Supón ahora que Ana elige $a = 6$ y Beatriz $b = 7$. ¿Hay algún problema? ¿Puedes sugerir como resolverlo? (Intenta que tu solución funcione en situaciones similares que puedan plantearse en otros casos.)

c) ¿Hay algún problema si Ana elige $a = 4$ y Beatriz $b = 7$? ¿Es del mismo estilo que el problema anterior? ¿Puedes resolverlo? (Intenta de nuevo que tu solución funcione en situaciones similares que puedan plantearse en otros casos.)

b) Cristina intercepta un mensaje "18" que Ana la envía a Beatriz y un mensaje "8" enviado por Beatriz a Ana. A continuación intercepta el mensaje *ELHQKHFKR* de Ana a Beatriz. ¿Qué le ha dicho Ana a Beatriz?

2. En la guía de una red de comunicaciones aparece la siguiente información:

ESTRUCTURA GENERAL: Los mensajes se cifrarán mediante el criptosistema R.S.A.. Se utilizará el alfabeto castellano de 26 letras (con Ñ y sin W). Las unidades de texto normal serán digrafos y las de texto cifrado trigrafos. Los mensajes se mandan firmados (usando el protocolo explicado en clase).

CLAVES DE LOS USUARIOS ..... (n, e)

Usuario A ..... (9797,17)

Usuario B ..... (8549,6083)

etcétera

El usuario A envía un mensaje al usuario B y lo termina con la firma EOBIXD. ¿Cómo se llama el usuario A?

3. En la guía de una red de comunicaciones aparece la siguiente información:

ESTRUCTURA GENERAL: Los mensajes, escritos en el alfabeto castellano de 27 letras (con Ñ y W) con los equivalentes númericos habituales ($A = 0, \dots, Z = 26$), se cifrarán mediante el criptosistema de El Gamal sobre el cuerpo finito $\mathbb{F}_{733} (= \mathbb{Z}/733\mathbb{Z})$, y se utilizará $g = 7$ como generador de $\mathbb{F}_{733}^*$. (Nota para el lector interesado: 2, 3 y 5 NO son generadores de $\mathbb{F}_{733}^*$.) Las unidades de texto en claro serán digrafos, pero para evitar inconvenientes que se discutirán luego, en lugar de hacer lo habitual, $XY = X \cdot 27 + Y$, sumaremos 1 a esta cuenta: $XY = X \cdot 27 + Y + 1$. De este modo el conjunto de mensajes en claro es $\{AA = 1, \dots, ZZ = 729\} \subset \mathbb{F}_{733}$. Todas las unidades de un mensaje se cifrarán con la misma clave, es decir, para comunicar el mensaje $N_1 N_2 N_3 \dots$ al usuario A se le enviará $(g^k, N_1 e_A^k, N_2 e_A^k, N_3 e_A^k, \dots)$. Este mensaje se enviará como números.

CLAVES DE LOS USUARIOS ..... $e (= g^d)$

Usuario A 556

Usuario B 369

etcétera

a) Comprueba que no habría ninguna dificultad para usar el sistema si se utilizase la convención usual para digrafos, $XY = X \cdot 27 + Y$, pero que en ese caso AA se cifraría siempre como 0, lo que sería una debilidad del sistema. Pon un ejemplo de un mensaje en el que aparezca el digrafo AA.

b) El usuario A, cuya clave secreta es $d_A = 12$, recibe de B el mensaje $(654, 449, 549)$. ¿Qué le ha dicho B?
c) Ahora A quiere decirle SI a B. Elige como exponente para cifrar el mensaje $k = 8$. ¿Qué debe enviarle a B?
d) B ha sido descuidado y le ha dicho a A que ha utilizado como exponente secreto d_B un número menor que 10. ¿Cómo es d_B?

4. Una de las claves para que RSA funcione es el siguiente resultado: si $n = pq$, con p, q primos distintos, y $ed \equiv 1 \pmod{phi(n)}$, entonces $(m^e)^d \equiv m \pmod{n}$ para cualquier entero m.
Sea ahora $N = \text{mcm}(p-1, q-1)$ [mcm=mínimo común múltiplo]. Demuestra que si $ed' \equiv 1 \pmod{N}$, entonces $(m^e)^{d'} \equiv m \pmod{n}$ para cualquier entero m.

5. Sea $n = pq$ con p y q primos impares y definimos

$$\lambda(n) = \frac{(p-1)(q-1)}{mcd(p-1, q-1)}.$$

Supngo que modificamos el RSA de juguete requiriendo que $ed = 1 \pmod{\lambda(n)}$.
a) Demuestra que con estas condiciones $Enc(m) = m^e \pmod{n}$ y $Dec(c) = c^d \pmod{n}$ son funciones inversas una de la otra.
b) Si $p = 37$, $q = 79$ y $e = 7$ encuentra d en este criptosistema modificado y en el RSA de juguete original.

6. Encontrar la clave privada de un usuario de un criptosistema basado en el RSA si su clave pública es $(7519, 35)$.

7. En la guía de una red de comunicaciones aparece la siguiente información:
ESTRUCTURA GENERAL: Los mensajes se cifrarán mediante el criptosistema RSA. Se utilizará el alfabeto castellano de 30 letras con 0,...,14,...,26=A,...,Ñ,...,Z, 27=el punto, 28=espacio en blanco y 29=la interrogación. Las unidades de texto normal serán digrafos y las de texto cifrado trigrafos.
CLAVES DE LOS USUARIOS ..... (n, e)
Usuario A ..... (1711,125)
etcétera

El usuario B envía el mensaje *ASÑAW.* al usuario A. ¿Qué quiere decirle B a A?

8. Supongamos que el alfabeto en claro tiene 29 letras con 0,...,26=A,...,Z [alfabeto castellano], 27=espacio en blanco, 28=el punto, y que el alfabeto cifrado tiene 30 letras, añadiendo al anterior 29=?. Las unidades de texto en claro serán digrafos vistos como números de dos cifras en base 29, es decir, enteros entre 0 y 840 [o elementos de $\mathbb{Z}/(841\mathbb{Z})$]. Análogamente, las unidades de texto cifrado serán digrafos vistos como enteros entre 0 y 899 [o elementos de $\mathbb{Z}/(900\mathbb{Z})$].

a) El cifrado de m es un entero $0 \leq f(m) \leq 850$ tal que

$$f(m) := m^{13} + 2 \pmod{851}.$$

(Notar que $(29)^2 < 851 < (30)^2$.) Descifra el mensaje *LFNÑ.*

b) ¿Es posible usar $g(m) := m^{11} + 2 \pmod{851}$ para cifrar?

9. Consideremos el espacio de textoplano $\mathcal{P} = \mathcal{U}(\mathbb{Z}/n\mathbb{Z})$. Diremos que m es fijo por el RSA de juguete si $Enc(m) = m^e \equiv m \pmod{n}$. Si $n = pq$ con p, q primos impares y $pk = (n, e)$, encontrar el número de $m \in \mathcal{P}$ fijos.

10. Supongamos que la clave pública de RSA es $pk = (317940011, 77537081)$ usa el ataque de Wiener visto en clase para encontrar la clave privada y factorizar n.

Dado un primo p, denotamos por $\mathbb{F}_p$ el cuerpo $\mathbb{Z}/p\mathbb{Z}$ y por $\mathbb{F}_p^*$ al grupo multiplicativo de las unidades i.e. $\mathbb{F}_p^* = \mathcal{U}(\mathbb{F}_p)$.
11. Cifra la palabra "CASA" usando el sistema ElGamal con $p = 997$, $g = 2$ y $h = g^d = 27$, utilizando como unidades de texto en claro digrafos en el alfabeto castellano de 27 letras (de la manera estándar) y como unidades de texto cifrado los elementos de $\mathbb{F}_{997}^* \times \mathbb{F}_{997}^*$ (sin convertirlos en letras). Encuentra la clave privada d y comprueba que el resultado es correcto.

12. El polinomio $x^3 + 2x^2 + 1$ es irreducible sobre $\mathbb{F}_3$ y por tanto $F_3[x]/(x^3 + 2x^2 + 1)$ es isomorfo a $\mathbb{F}_{3^3}$. Asociamos las 26 letras del alfabeto con los 26 elementos no cero de $\mathbb{F}_{3^3}$ usando el orden alfabético en las letras y el lexicográfico en los polinomios i.e.

A	B	C	D	E	F	G
1	2	x	$x+1$	$x+2$	$2x$	$2x+1$
H	I	J	K	L	M	N
$2x+2$	x^2	x^2+1	x^2+2	x^2+x	x^2+x+1	x^2+x+2
O	P	Q	R	S	T	U
x^2+2x	x^2+2x+1	x^2+2x+2	$2x^2$	$2x^2+1$	$2x^2+2$	$2x^2+x$
V	W	X	Y	Z	?	?
$2x^2+x+1$	$2x^2+x+2$	$2x^2+2x$	$2x^2+2x+1$	$2x^2+2x+2$	?	?

Supongamos que la clave publica es el grupo multiplicativo de $\mathbb{F}_{3^3}$ con la descripción dada arriba, el generador $g = x$, y el elemento $g^{11} = x^{11} \equiv x + 2 \pmod{x^3 + 2x^2 + 1}$.
Descifrar el siguiente mensaje:

$$(K, J)(P, U)(N, K)(N, R)(T, F)(V, Y)(E, H)(F, A)(T, W)(J, D)(U, J)$$

13. El Gamal hizo la siguiente propuesta de firma digital utilizando el logaritmo discreto sobre un cuerpo $\mathbb{F}_p$ con p un primo grande.
Paso 1) Todo el mundo se pone de acuerdo en un primo p y en un generador g de $\mathbb{F}_p^*$.
Paso 2) Ana (y todos los demás usuarios), elige un exponente d_A que mantiene secreto, y hace público $e_A \equiv g^{d_A} \pmod{p}$ (exáctamente como en el criptosistema de El Gamal).
Paso 3) Para enviar su firma (para ese mensaje), que viene dada por un número f, con $0 \leq f \leq p-1$, Ana elige al azar un número k tal que $(k, p-1) = 1$. Luego calcula $r \equiv g^k \pmod{p}$ y resuelve la ecuación $g^f \equiv e_A^r r^x \pmod{p}$ en la incógnita x. Finalmente Ana envía a Beatriz el par (r, x) junto a su firma f.
Paso 4) Beatriz comprueba que $g^f \equiv e_A^r r^x \pmod{p}$, y se asegura de que la firma f corresponde a Ana.
a) Comprueba que Ana conoce todo lo necesario para poder calcular x.
b) Comprueba que Beatriz conoce todo lo necesario para certificar la firma.
c) Comprueba que Cristina no puede hacerse pasar por Ana sin conocer d_A, es decir, sin resolver el problema del logaritmo discreto, y que por tanto Beatriz puede estar segura de que el mensaje procede de Ana.