Teoría de Códigos y criptografía
Curso 2009-2010

Hoja 4 (Criptografía asimétrica)

1. Se propone el siguiente sistema para jugar al poker por correo (el problema es como repartir las cartas sin que ninguno de los dos jugadores sepa las cartas que tiene el otro).

i) El jugador A pone cada una de las 52 cartas en una caja (todas las cajas son idénticas) y las cierra con candados para los que solo él tiene las llaves. Envía las 52 cajas al jugador B.

ii) El jugador B selecciona 5 de las cajas, que formarán la mano de A. Selecciona otras 5 cajas, que formarán su propia mano, y a estas 5 les pone candados para los que solo él tiene la llave. Envía las 10 cajas seleccionadas a A.

iii) A retira sus candados de las 10 cajas. Se queda con las 5 cartas que forman su mano y envía las otras 5 cajas a B.

iv) B abre las 5 cajas y ya tiene sus cartas. Pueden empezar a jugar.

v) En caso de disputa B envía sus 5 cartas y las 42 cajas sin abrir a un arbitro neutral, al que A le envía las llaves.

EJERCICIO: Convencerse de que no se pueden hacer trampas y dar un método para jugar al poker utilizando el correo electrónico.

2. En una red de comunicaciones cada usuario U tiene su función para cifrar C_U, que hace pública, y su función para descifrar D_U, que mantiene secreta. Un mensaje m del usuario A al usuario B se enviará siempre en el siguiente formato: $(C_B(m), A)$. La dirección A le indica a B quién ha enviado el mensaje. El receptor B recuperará m a partir de $(C_B(m), A)$, y también, de manera automática, contestará $(C_A(m), B)$ a A (observesá que $(C_A(m), B)$ tiene el formato adecuado). De esta manera A sabe que B ha recibido correctamente el mensaje.

a) Prueba que un tercer usuario C puede tambien leer el mensaje m que A envió a B. Podemos asumir que C puede interceptar todos los mensajes transmitidos por la red (ya que una de las ventajas de la clave pública es que elimina la necesidad de que el canal sea seguro), y que C puede enviar sus propios mensajes, siempre que utilice el formato correcto.

b) Demuestra que las comunicaciones utilizando esta red siguen sin ser seguras si el protocolo es que A envía $C_B((C_B(m), A))$ a B y B automaticamente responde $C_A((C_A(m), B))$ a A.

3. Al pagar con una tarjeta de crédito los usuarios (compradores y vendedores) deben comprobar una serie de cosas: el vendedor debe asegurarse de que la tarjeta es auténtica y tiene fondos, de que la tarjeta no es robada, de que el comprador no va a negar haber hecho la compra,...; por su parte el comprador debe asegurarse de que el vendedor no va a intentar cobrar de más o antes de tiempo, de que no va a utilizar posteriormente los datos de su tarjeta para hacer compras por su cuenta.... Para evitar todo esto se propone el siguiente sistema.

La autoridad emisora de las tarjetas (que llamaremos AE) elige una función de un sólo sentido, f que hace pública, manteniendo secreta la función inversa f^{-1}. Por su parte cada usuario i del sistema (comprador o vendedor) elige una serie de datos de identificación I_i y una función de un sólo sentido f_i (puede elegirla cada usuario por su cuenta siguiendo las instrucciones de la AE). El usuario i envía I_i a la AE, y ésta le devuelve $s_i = f^{-1}(I_i)$. Con estos datos i construye su credencial: (I_i, s_i, f_i), que hace pública, manteniendo secreta f_i^{-1}. Con todos estos datos, cuando el comprador i quiere pagar al vendedor j, siguen el siguiente protocolo:

i) *Presentación de credenciales:* El comprador entrega al vendedor (I_i, s_i, f_i) junto con una descripción de la transacción (pago, fecha de cobro,...) desde su punto de vista: u_i. El vendedor comprueba si $f(s_i) = I_i$, y acepta o no la tarjeta. Se procede de manera simétrica entregando el vendedor sus datos, (I_j, s_j, f_j, u_j), al comprador.

ii) *Autentificación:* El comprador y el vendedor unen (de modo adecuado dependiendo del tipo de funciones que se use) u_i y u_j, creando un $u = u_i u_j$. El comprador calcula $t_i = f_i^{-1}(u)$ y se lo da al vendedor, quién comprueba si $f_i(t_i) = u$. Se realiza la operación simétrica intercambiando los papeles de comprador y vendedor.

iii) *Recibos:* el comprador guarda $(I_j, s_j, f_j, u_i, u_j, t_i, t_j)$ y el vendedor guarda $(I_i, s_i, f_i, u_i, u_j, t_i, t_j)$.

EJERCICIO: Discute la utilidad de este sistema para resolver los problemas planteados en el primer parrafo, y cualquier otro que se te ocurra relacionado con los pagos con tarjeta de crédito.

4. 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, $\{A, \ldots, Z\}$ como las clases $\{1, \ldots, 27\} \subset (\mathbb{Z}/29)^*$, 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) Cristina intercepta un mensaje "7" que Ana la envía a Beatriz y un mensaje "9" enviado por Beatriz a Ana. A continuación intercepta el mensaje *ELHQKHFKR* de Ana a Beatriz. ¿Qué le ha dicho Ana a Beatriz?

5. Supongamos que una red de inversores y agentes de bolsa utiliza criptografía de clave pública. Los inversores temen que sus agentes compren acciones sin su autorización (para cobrar comisiones) y luego, si pierden dinero, digan que recibieron instrucciones de hacerlo (mostrando un mensaje cifrado con una indicación en ese sentido y pretendiendo que venía del inversor). Los agentes, por su parte, temen que, si compran acciones siguiendo las instrucciones del inversor y éstas pierden valor, el inversor pretenda que nunca dio la orden de compra y que el mensaje está falsificado por un tercero o por el propio agente.

Explica cómo puede la criptografía de clave pública resolver estos problemas de modo que cuando todos estos indeseables acaben ante los Tribunales demandándose unos a otros, haya una prueba de quién es el culpable de las malas inversiones y consecuente pérdida de dinero. Puedes suponer que, en caso de una demanda entre el inversor A y el agente B, se pone a disposición del juez toda la información para cifrar/descifrar, es decir, las claves e_A, d_A, e_B, d_B y el software necesario para cifrar y descifrar. [PISTA: hace falta un "acuse de recibo"de los mensajes.]

6. 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?

7. 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 30 letras con 0,...,26=A,...,Z [alfabeto castellano], 27=el punto, 28=espacio en blanco y 29=la interogación. 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 decir B a A?

8. Un grupo de espias decide cifrar sus mensajes, escritos en un alfabeto de 27 letras (las 26 del castellano, con Ñ y sin W, y un espacio en blanco "_"que cifrarán como el 26), utilizando un sistema de Vigenére sobre pares de letras. Para dificultar la labor del enemigo, y en particular el análisis de frecuencias, deciden cambiar la clave en cada mensaje. Para intercambiarse las claves acuerdan utilizar el sistema RSA de clave pública. El protocolo que utilizan es el siguiente:

Cuando A quiere enviar a B un mensaje m, busca una clave de Vigenére, K, que será un par de letras k_1k_2. Esta clave le da una función para cifrar g_K. Además B tiene una función pública para cifrar claves, f_B, cuya correspondiente función para descifrar, f_B^{-1}, es secreta. A interpreta K (en principio un par de letras) como un digrafo (un "número de dos cifras") al que puede aplicar f_B, y lo que envía a B es el par $(f_B(K), g_K(m))$. B puede recuperar K a partir de $f_B(K)$, y una vez que conoce K puede leer m a partir de $g_K(m)$.

a) Si las claves para cifrar son de la forma (n, e), ¿Hay alguna restricción sobre el tamaño de n?

b) Las primeras lineas de la guía de claves públicas para cifrar claves de Vigenére dicen:

Usuario A ..... $((3^9 - 1)/2, 3629)$

Usuario B ..... $((2^{15} - 1)/7, 643)$

El usuario B recibe el mensaje (AGR, TPXUROXK_X). ¿Qué le han querido decir?

c) Como acabas de comprobar, el protocolo anterior tiene un serio problema de autentificación: cualquiera podría haber enviado el mensaje. Discute si para resolver este problema es suficiente que cuando A escribe a B envie el mensaje en la siguiente forma: (Hola soy A, $f_A^{-1}(f_B(K)), g_K(m))$; o si hace falta introducir alguna firma adicional. Discute también si siempre se podrá utilizar $f_A^{-1}(f_B(K))$ o si habrá casos en los que convenga sustituirlo por $f_B(f_A^{-1}(K))$. ¿Introduce esta modificación alguna nueva restricción sobre el tamaño de las posibles n de las claves?

d) Supón que los espias han decidido cambiarse al nuevo protocolo descrito en c), y que quien envió el mensaje de b) fue A. ¿Como debería enviar ese mismo mensaje con el nuevo protocolo?

9. 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 $\mathbb{Z}/(900\mathbb{Z})$].

1. 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*.

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

10. 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 ($A = 0, \ldots, Z = 26$), se cifrarán mediante el criptosistema de El Gamal sobre el cuerpo finito $\mathbb{F}_{733}(= \mathbb{Z}/733)$, 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 $\{AA = 1, \ldots, ZZ = 729\} \subset \mathbb{F}_{733}$. Todas las unidades de un mensaje se cifrarán con la misma clave, es decir, para comunicar el mensaje $N_1N_2N_3\ldots$ al usuario A se le enviará $(g^k, N_1e_A^k, N_2e_A^k, N_3e_A^k, \ldots)$. 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?

11. 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 $e_A \equiv g^{d_A} \mod p$ (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 $r \equiv g^k \mod p$ y resuelve la ecuación $g^f \equiv e_A^r r^x \mod p$ en la incógnita x. Finalmente Ana envía a Beatriz el par (r, x) junto a su firma f.

Paso 4) Beatriz comprueba que $g^f \equiv e_A^r r^x \mod p$, 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.

12. El objetivo de este problema es dar un método para lanzar una moneda al aire "a distancia" usando una función 2-a-1 de un sólo sentido. Por ejemplo, para que dos personas que juegan al ajedrez por internet puedan acordar quién lleva las blancas.

Un sistema de funciones 2-a-1 de un sólo sentido es un algoritmo que, dada una clave e, construye una función $f : \mathcal{M} \longrightarrow \mathcal{C}$ tal que cada elemento $c \in Im(f)$ tiene exactamente dos preimágenes m_1, m_2 tales que $f(m_i) = c$; junto a a otro algoritmo que, dada una clave d que "invierte e", puede encontrar las dos preimágenes de cualquier $c \in Im(f)$. Suponemos ademas que es computacionalmente imposible encontrar d conociendo sólo e. Observa que, dado $m_i \in$

$\mathcal{M}$, podemos encontrar el otro elemento m_2 tal que $f(m_1) = f(m_2)$ si conocemos tanto e como d; pero estamos asumiendo que, conociendo sólo e, es computacionalmente imposible calcular el compañero m_2 de ningún m_1.

Supongamos que Ana y Beatriz quieren utilizar esto para "lanzar una moneda al aire". Ana genera un par de claves (e, d) y envía e, pero no d, a Beatriz. Encuentra un procedimiento en el que cada jugadora tenga una probabilidad del 50 % de "ganar" (empieza por dar una definición adecuada de "ganar") y que incluya garantías de que no se puede hacer trampas.

13.

a) Sea R un dominio de integridad [es decir, $ab = 0 \Rightarrow a = 0$ ó $b = 0$] y consideremos soluciones de ecuaciones en R. Demostrar que la ecuación $X^2 = 0$ tiene exactamente una solución. Ver que si $a \neq 0$, la ecuación $X^2 = a$ tiene a lo sumo dos soluciones. Si además suponemos que $2 \neq 0$ en R, demostrar que, si $X^2 = a$ con $a \neq 0$ tiene solución, entonces tiene exactamente dos soluciones.

b) Sea N un número impar. Demostrar que en el anillo $\mathbb{Z}/N\mathbb{Z}$ existe algún a tal que la ecuación $X^2 \equiv a \mod N$ no tiene ninguna solución. (Sugerencia: ¿Cardinal del conjunto de cuadrados?)

c) Demostrar que en el anillo $\mathbb{Z}/p^2\mathbb{Z}$ con p primo impar la ecuación $X^2 \equiv 0 \mod p^2$ tiene exactamente p soluciones, mientras que si una ecuación $X^2 \equiv a \mod p^2$ con $a \not\equiv 0$ tiene solución, entonces tiene exactamente dos soluciones.

d) Sean p y q primos impares distintos. Trabajaremos ahora en el anillo $\mathbb{Z}/pq\mathbb{Z}$.

d1) Demostrar que, dado $x \in \mathbb{Z}/pq\mathbb{Z}$, existen $a, b \in \mathbb{Z}$, $\quad 0 \leq a < q, \quad 0 \leq b < p$ tales que $x \equiv ap + bq \mod pq$, y que además a y b en estas condiciones son únicos.

d2) Dados $x \equiv ap + bq, x' \equiv a'p + b'q \in \mathbb{Z}/pq\mathbb{Z}$, dar condiciones sobre a, b, a', b' que sean equivalentes a $x^2 \equiv x'^2 \mod pq$.

d3) Lo mismo que en d2), pero exigiendo además que $x \not\equiv x' \mod pq$.

d4) Demostrar que la ecuación $X^2 \equiv \alpha^2 \mod pq$ tiene: 1 solución si $\alpha \equiv 0 \mod pq$; 4 soluciones si α es una unidad en $\mathbb{Z}/pq\mathbb{Z}$; 2 soluciones si $\alpha \not\equiv 0$ y α no es una unidad en $\mathbb{Z}/pq\mathbb{Z}$.

14. Supongamos que tenemos un método rápido [existen algunos probabilísticos] para resolver la ecuación $X^2 \equiv a \mod p$ cuando p es primo y existe solución [esto es, a es un *residuo cuadrático* módulo p]. Supongamos también que si n es compuesto y producto de dos primos distintos, $n = pq$, no hay forma razonable de resolver $X^2 \equiv a \mod n$ que no pase por factorizar n (en cuyo caso podemos resolver $X^2 \equiv a \mod p$ y $X^2 \equiv a \mod q$ y utilizar el Teorema Chino del Resto). Supongamos por último que p y q no son ambos $\equiv 1 \mod 4$.

Sea $K_e = n$ y sea $K_d = \{p, q\}$ su factorización. Pongamos $\mathcal{P} = \mathcal{C} = (\mathbb{Z}/n)^*/\{\pm 1\}$, esto es identificamos cada clase inversible x con su opuesta $-x$, y consideremos la función $f : \mathcal{P} \to \mathcal{C}$ definida por $f(x) = x^2$. Demuestra que todo esto es un ejemplo de la situación descrita en el problema 12 y que por tanto acabamos de dar una forma explícita de lanzar monedas al aire "a distancia".