1 RSA

- $p = 11$, $q = 7$, $d = 53$ $\Rightarrow$ $(77, 17)$
- $(119, 5)$, $E = 81$ $\Rightarrow$ $m = 30$
- $(65, 7)$, $E = 31$ $\Rightarrow$ $m = 21$
- $(299, 5)$ $\Rightarrow$ $p = 13$, $q = 23$, $d = 53$
- No se puede afirmar que calcular d a partir de (n, e) sea polinomial.

2 Curvas Elípticas

- Si tomamos una c.e. módulo p dada en forma de Weierstrass $\Rightarrow$ El número de puntos de la c.e. está comprendido en el intervalo $[(\sqrt{p}-1)^2, (\sqrt{p}+1)^2]$.
- (V/F) Una c.e. sobre un cuerpo K tiene siempre un punto proyectivo con coordenadas enteras.
- (V/F) Tres puntos alineados de una c.e. siempre suman cero.
- Si $E(\mathbb{F}_{p^k})$ es el grupo de una c.e. $\Rightarrow$ Si es cíclico, no puede tener más de un elemento de orden dos.
- Sea $\mathbb{F}_{2^{233}}$. ¿Por qué no es bueno emplear la ecuación $y^2 + (\xi^{221} + \xi^{120})y = x^3 + x + \xi^{3122}$? $\Rightarrow$ Porque es supersingular.

2.1 Menezes-Vanstone

- Sobre $\mathbb{F}_{11}$ utilizamos la curva $y^2 = x^3 + 2x + 5$ y el punto $Q = (9, 2)$, clave privada $a = 3$ y su clave pública $aQ = (8, 4)$. ¿Cuál NO puede ser cifrado del mensaje $(5, 5)$? $\Rightarrow$ $((9, 2), 9, 7)$
- Sobre $\mathbb{F}_{41}$ utilizamos la curva $y^2 = x^3 + 33x + 35$ y el punto $Q = (8, 27)$, clave privada $a = 21$ y su clave pública $aQ = (6, 3)$. ¿Cuál SI puede ser cifrado del mensaje $(32, 22)$? $\Rightarrow$ $((19, 10), 35, 33)$
- Sobre $\mathbb{F}_{16}$ utilizamos la curva $y^2 + xy = x^3 + (\xi^3 + \xi + 1)x^2 + \xi^3 + \xi$ y el punto $Q = (\xi^3 + \xi^2 + \xi + 1, \xi^2 + 1)$, clave privada $a = 3$ y su clave pública $aQ = (\xi^3 + \xi^2 + \xi, \xi^3 + \xi^2)$. Obtenemos el criptograma $((\xi^3 + \xi^2 + \xi + 1, \xi^3 + \xi), \xi^3 + 1, \xi^3 + \xi + 1)$ ¿Cuál es el mensaje? $\Rightarrow$ $(\xi^3, \xi^3 + \xi^2)$
- Sobre $\mathbb{F}_{17}$ utilizamos la curva $y^2 = x^3 + x + 1$ y el punto $Q = (0, 1)$, clave privada de B es $a = 3$ y la clave pública de A es $aQ = (15, 5)$. Clave compartida: $\Rightarrow$ $(10, 5)$

3 Primos de Fermat

- (V/F) Un pseudoprimo de Fermat, $n = psp(a)$, satisface $a^{n-1} \equiv 1 \pmod{n}$ y es compuesto.
- (V/F) Los pseudoprimos fuertes pueden certificar que un número es compuesto pero no que es primo.
- (V/F) Aunque sea fácil comprobar la primalidad de un número de Fermat puede ser dificil demostrar la primalidad de alguno de sus factores.

- (V/F) Un pseudoprimo de Euler respecto de la base a es siempre pseudoprimo de Fermat respecto de la misma base.
- (V/F) Sólo se conocen un número finito de números de Carmichel.
- (V/F) Los tests de Solovay-Strassen y el de Miller-Rabin pueden certificar que un número es compuesto.

4 FCS

- La FCS de $\sqrt{d}$ con d libre de cuadrados es $[q_0, \dots, 2q_0]$ donde cada $q_i < q_0$.
- Si $\alpha = \frac{P+\sqrt{d}}{Q}$ es un irracional cuadrático (d libre de cuadrados):
  - La FCS de α es periódica con periodo máximo $2d-1$.
  - La FCS de α es puramente periódica sii $\alpha > 1$ y $1 < \overline{\alpha} < 0$ (su conjugado).
- (V/F) Una FCS finita coincide con su último convergente.
- Si $x^2 - dy^2 = N$ ($|N| < \sqrt{d}$) es una ecuación de Pell $\Rightarrow$ Cualquier solución positiva con $mcd(x,y) = 1$, son el numerador y el denominador de una convergente de la FCS de $\sqrt{d}$.
- $\alpha = \sqrt{2} \Rightarrow \alpha = [1, 2, 2, \dots]$
- $\alpha = \sqrt{3} \Rightarrow$ No es puramente periódica.
- $\alpha = \frac{a+\sqrt{a^2+4}}{2} \Rightarrow \alpha = [a, a, a, \dots]$
- $\alpha = \frac{1+\sqrt{5}}{2} \Rightarrow \alpha = [1, 1, 1, \dots]$
- (V/F) $\sqrt{a^2-1} = [a-1, \overline{1, 2(a-1), \dots}]$

5 Diffie-Hellman

- $p = 73$, $g = 5$. Claves públicas $A = (p, q, 37)$ y $B = (p, q, 12)$. Clave compartida $\Rightarrow$ 32.
- $p = 37$, $g = 2$. Clave pública $A = (p, q, 3)$ y clave compartida 10. Clave privada B $\Rightarrow$ 30.

6 ElGamal

- Cuál de las siguientes parejas NO puede ser el cifrado de $m = 10$ con ElGamal y clave privada $a = 4$ con parámetros:
  - $p = 23$, $g = 5 \Rightarrow 14, 7$
  - $p = 17$, $g = 3 \Rightarrow 14, 7$

7 Logaritmo Discreto

- ¿Cual de los algoritmos NO se puede emplear para el cálculo de log. dis. en $\mathbb{F}_{2^{1024}}$? $\Rightarrow$ Cálculo de índice en cuerpos primos.
- Aplicamos SIlver-Pohlig-Hellman para el cálculo de log. dis. de un elemento b de orden $n = 700$. ¿Cuántas raíces de la unidad en $< b >$ hay que calcular? $\Rightarrow$ 14.

8 Raíces cuadradas

- ¿Qué γ puede usarse para calcular la raíz de 27 módulo 37? $\Rightarrow$ $\gamma = 18$.
- ¿Cuál de esto enteros no tiene raíz cuadrada módulo 53? $\Rightarrow$ 30.

9 Modos

- ECB. El que menos bits cambia en el criptograma cuando alteramos un bit en el mensaje.
- CBC. Ninguna de las otras opciones.
- OFB. Convierte un cifrado de bloque en un cifrado de flujo síncrono.
- CFB. Convierte un cifrado de bloque en un cifrado de flujo autosincronizable.

10 Teoría

- Integridad: La información no ha sido alterada en el envío.
- No repudio: El emisario no puede negar haber realizado el envío.
- Autenticidad: La información proviene de quien dice enviarla.
- Confidencialidad: La información sólo puede ser accesible por las entidades autorizadas.
- Cifrado de flujo síncrono. Es más vulnerable que un cifrado de flujo autosincronizable al cambio de un carácter en el criptograma.
- Criptosistema de clave pública. No podemos $\Rightarrow$ ninguna de las tres opciones.

11 Preguntas sueltas

BABY STEP Sea G un grupo, $b \in G$ de orden 101. en BS-GS el número máximo de elementos de G que necesitamos tener almacenados es $\Rightarrow$ 13.

PRATT (V/F) El certificado de Pratt es recursivo y usa el concepto de orden multiplicativo módulo n.

MONTECARLO (V/F) El test probabilístico tipo Montecarlo corre en tiempo polinomial y puede ser inclinado a TRUE, a FALSE o no inclinado.

LUCAS-LEHMER (V/F) Existe un n no primo con el grupo multiplicativo de las unidades módulo n cíclico.

EC. CUADRÁTICA ¿Cuál en $\mathbb{F}_{32}$ tiene solución? $\Rightarrow$ $z^2 + (\xi^3 + \xi)z + (\xi^3 + \xi^2)$

LAS VEGAS (V/F) Un test probabilístico tipo Las Vegas produce una respuesta correcta en tiempo aleatorio cuya media está acotada polinomialmente.