Practico 5 de Criptografia-2007

1): Encuentre $mcd(7469, 2464)$ y $mcd(2689, 4001)$.

2): Calcular el máximo común divisor y expresarlo como combinación lineal entera: a) 14 y 35. b) 11 y 15.

3): Hallar las cifras de las unidades y de las decenas de $7^{15343287951}$, $7^{374567838}$, $7^{735683450327833751351367 81}$ y de $7^{3783456783657568752}$

4): Hallar el resto de la división de $11^{9595895093}.13^{9859340590021}$ por 12

5): Resolver las siguientes ecuaciones.

a) $3x \equiv 1(5)$ b) $2x \equiv 5(6)$ c) $35x \equiv 14(182)$ d) $10x \equiv 2(22)$

6): (ejercicio de calculo de RSA, con primos ridiculamente pequeños) Tomar $p = 5$, $q = 17$, esto da un tamaño de bloque de 6 bits.

a) Tomar como clave publica $e = 3$. Encriptar 100101001010010010100010101001 . Observar el extraño comportamiento del cuarto bloque. Observar que para desencriptar, no se puede volver a colocar el ciphertext como bloques de 6 bits.

b) Cambiar el ultimo bit (el de mas a la derecha) en cada bloque, y reencriptar. (Observar que a veces las diferencias con el primer encriptado son significativas, pero a veces no. Tambien observar el extraño comportamiento, otra vez, del cuarto bloque).

c) Ahora, cambiar el primer bit (el de mas a la izquierda) del original (de a)), y repetir. Observar que ahora si hay diferencias, pero esta vez el tercer bloque se comporta en forma rara.

d) Calcular la clave privada d. (chequeo: encriptando d, se obtiene el numero 32).

e) Desencriptar 10,2,68,54,11. Observar la relacion entre el segundo bloque de este item y el cuarto bloque de c).

7): Tomar $p = 7$, $q = 5$. Tomar cualquier numero que Ud. quiera como clave publica e. (Recuerde que puede ser cualquiera, siempre que sea coprimo con $(p-1)(q-1)$). Calcular d y sorprenderse de la respuesta. Repetir, si quiere.

8): (ejercicio de desencriptamiento de RSA, usando primos ridiculamente pequeños). Eva intercepta un mensaje cifrado $c = 3650502$ enviado a A. Eva sabe que la clave publica de A es $n = 6012707$, $e = 3674911$.

Factorice n, encuentre la clave privada d de A, y desencripte c. Verifique el resultado encriptando c.

9): Sea $n = 16199$. Se sabe que el ciphertext es:

14238, 7052, 4454, 2444, 2684, 14560, 0, 3314, 11500, 14238, 2684, 10952.

Descifrar el mensaje, interpretando que $A = 00$, $B = 01$, ..., $Z = 25$.

10): Un ataque contra RSA, llamado el algoritmo de factorizacion de Pollard, factoriza $n = pq$ si $p - 1$ (o $q - 1$) es divisible solo por primos "pequeños". Otro ataque, de Wiliams, factoriza n si $p + 1$ es el que es divisible solo por primos "pequeños". Algunos criptografos recomiendan entonces el uso de "primos fuertes" en RSA. Un primo p es fuerte si:

1) $p - 1$ es divisible por un primo "grande" r.

2) $p + 1$ es divisible por algun primo "grande".

3) $r - 1$ es divisible por algun primo "grande".

(1) proteje contra Pollard, 2) contra Williams, y 3) contra los ataques ciclicos). Otros opinan que no es necesario construir deliberadamente primos fuertes, pues si p y q son elejidos al azar y suficientmente grandes, las probabilidades de que $p - 1$ y $p + 1$ tengan algun primo grande que los divida son altas, y, por otro lado, el ataque ciclico no tiene muchas probabilidades de tener exito. Ademas, el uso de primos fuertes no brinda ninguna proteccion contra el algoritmo de factorizacion por curvas elipticas, por ejemplo. Por otro lado, crear primos fuertes no es mucho mas dificil que crear primos comunes:

Algoritmo de Gordon para generar un primo fuerte p:

1. Generar dos primos s y t "grandes", de aproximadamente la misma longitud.
2. Elejir un entero i_0, y tomar como r el primer primo en la sucesion $2it + 1$ con $i = i_0, i_0 + 1, \ldots$.
3. Calcular $s_0 := s^{r-2} \bmod r$, y $p_0 := 2s_0 s - 1$.
4. Elejir un entero j_0, y tomar p el primer primo en la sucesion $p_0 + 2jrs$ con $j = j_0, j_0 + 1, \ldots$.

Probar que el algoritmo de Gordon produce un primo fuerte.