Practico 3 de Criptografia-2007

1): Probar que la función $X \mapsto X(2X+1)$ usada en RC6 es biyectiva. (las operaciones son modulo 2^{32}).

2): Tomar alguno (o varios, si quiere) de los S-boxes de Serpent (leer el paper en mi pagina) y encontrar una representación del mismo con operaciones booleanas.

3): Escribir un programa que tome como input un S-box y le calcule la tabla de diferencias y la maxima diferencia, y la tabla de probabilidades lineales y la mayor probabilidad lineal.

Observar que hacer lo primero es mucho mas rápido que lo segundo.

4): Tomar los S-boxes de Serpent, y aplicarle los programas del ejercicio anterior.

5): *Verificar que la matriz de difusión de Rijndael es realmente MDS. (*: este ejercicio requiere alguna idea de cuerpos finitos, al menos de como programar las operaciones del cuerpo. El cuerpo finito que usan los de Rijndael esta implementado como $\boldsymbol{Z}_2[x]/m(x)$, donde $m(x) = x^8 + x^4 + x^3 + x + 1$).

Para los proximos ejercicios, se usara el cifer de 16 bits dado como ejemplo en clase, ver el tutorial de DC/LC para mas datos.

6): Calcular la probabilidad de la caracteristica $(\Delta X_1, \Delta X_2, \Delta X_3, \Delta X_4)$ donde X_i es el texto al principio de la ronda i, dada por:

$$\begin{aligned}\Delta X_1 &= 1011\ 0000\ 1011\ 1011\\ \Delta X_2 &= 0000\ 0000\ 1011\ 0000\\ \Delta X_3 &= 0000\ 0000\ 0010\ 0000\\ \Delta X_4 &= 0000\ 0010\ 0000\ 0010\end{aligned}$$

7): Repetir el punto anterior con la caracteristica:

$$\begin{aligned}\Delta X_1 &= 1000\ 0000\ 1000\ 0000\\ \Delta X_2 &= 1010\ 0000\ 1010\ 1010\\ \Delta X_3 &= 1011\ 0000\ 0000\ 0000\\ \Delta X_4 &= 0000\ 0000\ 1000\ 0000\end{aligned}$$

8): Calcule la probabilidad de las "mejores" caracteristicas de tres rondas, (i.e., que abarquen desde el principio de la primera hasta el principio de la cuarta) que pueda hallar que empiezen con la diferencia 1011 en un S-box y 0000 en los otros. (en clase dimos la que empezaba con esa diferencia en el S-box 2. Hacer los otros tres casos).

9): Repetir el ejercicio anterior, pero ahora usar mascaras lineales y probabilidades lineales en vez de diferencias y probabilidades dioferenciales.

10): Repetir el anterior pero con la mascara 1000 en un S-box y 0000 en los otros

11): Busque alguna diferencia y alguna mascara de entradas que crea que le puede dar una buena probabilidad diferencial o lineal, y calculelos.

12): Ahora tomaremos un cifer de 64 bits: sera como el anterior, pero ahora tendremos 16 S-boxes en vez de solo 4. La permutacion de bits en cada ronda es la siguiente: agrupamos los 64 bits en 4 palabras de 16 bits cada una. Dentro de cada palabra le hacemos la permutacion del cifer anterior. (ie.el bit i del S-box j lo mandamos al bit j del S-box i). Luego de hacer esto, mandamos el nibble i de la palabra j al nibble j de la palabra i.

Probar que comenzando con la diferencia 1011 en el segundo S-box y 0000 en las otras, obtenemos un ataque que es capaz de encontrar 24 bits de la clave de whitening con solo 86 (chosen) textos.

13): Ahora, repetir el ataque usando las diferencias de entrada 1011 0000 1011 1011 en la palabra i y 0 en las otras palabras. (Hacer todos los casos)

14): Usar LC contra el cifer anterior.

15): En una ronda de un cifer Feistel, digamos $L' = L \oplus F(R)$, si tenemos una diferencia asociada a L, digamos ΔL y una asociada a $F(R)$, digamos ΔF, entonces $\Delta L' = \Delta L \oplus \Delta F$. Sin embargo, esto no ocurre con mascaras: dada una mascara Γ_L y una mascara Γ_F, no es cierto en general que $\Gamma_{L'} = \Gamma_L \oplus \Gamma_F$.

a) Explicar con un ejemplo porque esto no es cierto.

b) Probar que en realidad lo que vale es que dado $\Gamma_{L'}$, conviene tomar $\Gamma_L = \Gamma_F = \Gamma_{L'}$.

16): Consideremos un cifer igual a RC5, excepto que la mezcla con la clave es con $\oplus$ en vez de $+$. Es decir, la funcion de ronda es: $A = ((A \oplus B) <<< B) \oplus K_r$. ($A$ y B de 32 bits).

Numeremos los bits como bit32,bit31,....,bit1. Probar que si Δ es cualquier vector de 32 bits, con los bits 1,2,3,4,5 iguales a cero, entonces se tiene una caracteristica diferencial de tres rondas que empieza y termina con la diferencia (de 64 bits) $(\Delta, 0)$, y que tiene una probabilidad diferencial igual a 2^{-10}, la cual, por lo tanto, se puede iterar para obtener por ejemplo una probabilidad diferencial de 15 rondas de 2^{-50}, con lo cual se pueden atacar 16 rondas de este RC5 modificado.

17): En el caso del cifer anterior, probar que se puede montar un ataque de LC, usando por ejemplo una mascara de entrada $(00...00, 0....01)$, que queda igual luego de tres rondas. Calcular su probabilidad lineal.