Universidad Rey Juan Carlos

Grado en Ingeniería de la Ciberseguridad

Criptografía

Ejercicios prácticas autodirigidas. Bloque 3. Cifrado Asimétrico.

---

1. Considera el siguiente esquema de intercambio de claves *a la* Diffie-Hellman, pero con matrices. Alice elige una matriz A (con elementos sobre, por ejemplo $\mathbb{Z}_p^*$, para p un primo grande) y calcula una inversa generalizada de A, que llamaremos A^g (es decir, A^g cumple que $AA^gA = A$) y envía a Bob A^gA. Bob elige una matriz B (también con entradas en $\mathbb{Z}_p^*$) calcula una inversa generalizada de B, B^g y envía a Alice A^gAB y A^gABB^g. Finalmente, Alice envía a Bob ABB^g. Ambos pueden así calcular la clave secrete, AB ,

   - Comprueba que el esquema anterior es correcto
   - Supón que alguna de las matrices que se envían en el canal es invertible. Analiza la seguridad del esquema (frente a un adversario pasivo).

2. Si elegimos un módulo RSA $N = 3337$, da opciones adecuadas e, d para completar la generación de claves.

3. Considera una modificación del esquema de cifrado de Bellare y Rogaway en la que el cifrado de un texto m conste de tres componentes:

   - $F(r)$, con r aleatorio y F una función *one-way*,
   - $m \cdot F(r)$,
   - $H(m)$, con H un oráculo aleatorio

   Analiza informalmente la seguridad del esquema resultante.

4. Considera un esquema de cifrado de clave pública en el que el cifrado de un texto m conste se construya como $(f(r), H(m) \oplus r)$, donde f es una función de una vía (que transforma cadenas de bits en cadenas de bits del mismo tamaño, ℓ), H es una función hash (con rango en $\{0,1\}^\ell$) y r es una cadena aleatoria de ℓ bits que se genera *fresca* cada vez que invocamos al algoritmo de cifrado. Analiza informalmente esta construcción.

5. Vamos ahora a considerar un esquema de cifrado que utiliza polinomios (cuyos coeficientes estarían en un cuerpo finito). Supongamos que la clave pública es un polinomio de grado n, $p(x) = a_0 + a_1x + a_2x^2 + \cdots$. La clave secreta es una raíz r de p, es decir, $p(r) = 0$. El parámetro de seguridad fija el tamaño de los coeficientes y el grado del polinomio (por ejemplo, si ℓ es el parámetro de seguridad trabajamos en un cuerpo de "más o menos"ℓ elementos y p tiene grado polinomial en ℓ). El cifrado de un mensaje m se construye eligiendo un polinomio q al azar (con coeficientes aleatorios en el cuerpo finito dado), y de grado n, y luego construyendo el cifrado como

   $$c := p(x)q(x) + m.$$

   Describe cómo se realizaría el descifrado. Analiza la seguridad de esta construcción contestando, al menos, las siguientes preguntas:

   a. ¿Qué es necesario pedir en la elección de las claves, para que pueda haber seguridad de tipo *one-way*?

   b. ¿El diseño actual, con algún tipo de generación de claves, puede ser IND-CCA2?