xFranv8
www.wuolah.com/student/xFranv8
121

FinalMayoesqSOL.pdf

TRANSPARENCIAS DE TEORIA

1º Criptografía

Grado en Ingeniería de la Ciberseguridad

Escuela Técnica Superior de Ingeniería Informática. Campus de Móstoles
Universidad Rey Juan Carlos

Universidad Rey Juan Carlos

CRIPTOGRAFÍA - MAYO 2019
GRADO EN INGENIERÍA DE LA CIBERSEGURIDAD CURSO 2018-19

El examen se puntúa sobre un máximo de 8 puntos. Las respuestas no justificadas se considerarán NO CONTESTADAS.

PRIMER PARCIAL (5O MINUTOS)

1. (2 pts.) Verdadero o falso. Razona tu respuesta.

   a. La clase de complejidad P está contenida en la clase NP.

   b. El modo de operación CBC define el cifrado del bloque i-ésimo como

   $$c_i := m_i \oplus F(c_{i-1}),$$

   siendo m_i el i-ésimo bloque de texto claro y F el cifrador utilizado.

   c. Un generador pseudoaleatorio es una función que se utiliza para construir cifradores en bloque.

   d. Las variantes (iterados) del DES son esquemas menos seguros que el DES original, pero más eficientes.

2. (1 pt.) Estudia la resistencia a colisiones (CR) de la función hash construida con el siguiente procedimiento: dada una cadena de bits de entrada, $x = b_n b_{n-1} \cdots b_0$, si z es el entero que representa la cadena x (codificación binaria habitual), se calcula $2z + 2^{25}$, se escribe de nuevo en binario, obteniendo una cadena w y se define el hash $H(x)$ tomando los 8 bits más bajos (menos significativos) de w.

3. (1 pt.) Describe el proceso de cifrado y descifrado asociado a un cifrador en bloque F usado en modo CTR. Supongamos se envía un mensaje de 5 bloques, y que al transmitir el bloque 3 de texto cifrado c_3 se produce un error (y al receptor le llega, en lugar de c_3, otra cosa $\hat{c}_3$. ¿Cuáles de los 5 bloques podrán ser descifrados correctamente por un receptor legítimo?

1. (2 pts.) Verdadero o falso. Razona tu respuesta.

   a. El esquema de intercambio de claves de Diffie-Hellman basa su seguridad en que dado un generador g de un cierto grupo cíclico, y un exponente, $a \in \mathbb{N}$, es difícil de calcular el elemento g^a.

   b. El *dealer* del esquema de compartición de secretos de Shamir construye un polinomio de grado n para que $n-1$ usuarios sean suficientes para recuperar el secreto (que es el término independiente del polinomio).

   c. Un cifrado de clave pública NM-CPA es también IND-CPA.

   d. La firma RSA de libro de texto puede romperse con un "no-message attack".

2. (1 pt.) 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 mismo grado n, $p(x) = a_0 + a_1 x + a_2 x^2 + \cdots$. La clave secreta es una raíz r de p, es decir, $p(r) = 0$. 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?

3. (1 pt.) Supongamos que existe un esquema de firma digital con la propiedad de que dos usuarios distintos U_1 y U_2 son capaces de generar con sus claves secretas dos firmas idénticas σ de modo que, para todo mensaje m (que suponemos es un elemento de un cierto $\mathbb{Z}_p$ se tiene que (m, σ) es validado con la clave pública de verificación de U_1 y (m^2, σ) es validado con la clave pública de verificación de U_2. ¿Es este esquema seguro?

Universidad Rey Juan Carlos

Escuela / Facultad .....

Campus

TITULACIÓN:.....

ASIGNATURA:.....

D.N.I.:.....

APELLIDOS:..... NOMBRE:.....

FECHA:..... CURSO: ..... GRUPO:.....

ESQUEMA DE SOLUCIONES

[PARCIAL 1]

1 a) V si la solución de un problema de decisión puede obtenerse en tiempo polinomial, obviamente también se valida en tiempo polinomial

b) F ($c_j := F_k(m_j \oplus c_{j-1})$

c) F se usa para construir cifradores en FLUJO

d) F justo "al revés" : son algo más seguros y menos eficientes

2 Si $z = b_n \cdot 2^n + b_{n-1} 2^{n-1} + .. + b_0 \cdot 2^0$

y $n+1 < 25$, $2z + 2^{25} = 1 \cdot 2^{25} + b_n \cdot 2^{n+1} + \dots + b_0 \cdot 2 + 0 \cdot 2^0$

Así, $w = 1\,0\,\_\_\,0\, b_n\, b_{n-1} \cdots b_1 b_0 0$

Tomando $x = b_7\, b_6 \cdots b_0$ con $b_7, \dots b_0 \in \{0,1\}$, cualesquiera

$\bar{x} = \bar{b_7}\, b_6 \cdots b_0$

y $\bar{b_7} = 1 \oplus b_7$

$H(x) = b_6 \cdots b_0 \emptyset = H(\bar{x})$

$\Rightarrow$ no es CR

Universidad Rey Juan Carlos

Escuela / Facultad .....

Campus

TITULACIÓN:.....

ASIGNATURA:.....

D.N.I.:.....

APELLIDOS:..... NOMBRE:.....

FECHA:..... CURSO:..... GRUPO:.....

[3] 1) - Teoría.

Cifrado: Input $m_1 \| \ldots \| m_k$

$c_0 := IV$

$CTR := IV$

$c_i := m_i \oplus F(CTR + i) \quad (i = 1, \ldots, m_k)$

Output: $c_0 \| c_1 \| \ldots \| c_k$

Descifrado: Input: $c_0 \| \ldots \| c_k$

$CTR := c_0$

$m_i := c_i \oplus F(CTR + i) \quad (i = 1, \ldots, k)$

Output: $m_1 \| \ldots \| m_k$.

- Pregunta: todos los bloques de mensaje claro, salvo m_3, se recuperan sin problema (CTR es paralelizable)

Universidad Rey Juan Carlos

Escuela / Facultad .....

Campus

TITULACIÓN:.....

ASIGNATURA:.....

D.N.I.:.....

APELLIDOS:..... NOMBRE:.....

FECHA:..... CURSO: ..... GRUPO:.....

[PARCIAL 2]

[1 a) F se basa en la dificultad del problema del logaritmo discreto; dados g, g^a, calcular a

b) F hacen falta $n+1$ usuarios

c) V $NM \Rightarrow IND$ (en particular, esto se cumple en el escenario CPA)

d) V (visto en clase). A elige σ, calcula σ^e y el par (σ, σ^e) pasa la verificación

[2 . Descifrado; evaluar c (que es un polinomio!) en la clave secreta r, es decir

$$m := C(r)$$

. a) Debe ser difícil factorizar p. esto es, encontrar p t.q. $P(\beta) = 0$.

b) Nunca, pues, por ejemplo, es maleable. $c + \bar{m}$ es un cifrado válido de $m + \bar{m}$ (si c es un cifrado de m)

Universidad Rey Juan Carlos

Escuela / Facultad .....

Campus

TITULACIÓN:.....

ASIGNATURA:.....

D.N.I.:.....

APELLIDOS:..... NOMBRE:.....

FECHA:..... CURSO: ..... GRUPO:.....

3] Nunca es seguro: U_1 es capaz de firmar (en nombre de U_2) cualquier mensaje M cuya raíz cuadrada conozca.