xFranv8
www.wuolah.com/student/xFranv8


# EsqueSolParcial1.pdf

*EJERCICIOS-EXAMENES*

**1° 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
Grado en Ingeniería de la Ciberseguridad Curso 2018-19

*Esquema de soluciones*

---

## Primer Examen Parcial. Modelo A.

1. (1 pts.) Considera los modos de operación (CBC y CTR) para cifradores en bloque vistos en clase y responde las siguientes preguntas:

   a) ¿Cuáles de ellos pueden paralelizarse, es decir, para cuales podemos cifrar $n$ bloques de entrada $m_0, \ldots, m_n$ simultáneamente, y para qué otros hemos de hacerlo necesariamente de modo secuencial (y en el orden prescrito)?

   b) Si ciframos un texto $m_1, \ldots, m_7$ con un cifrador en bloque en modo CBC, y se produce un error en la trasmisión del cifrado del bloque $m_5$, (es decir, el emisor construyó $c_5$ pero el receptor recibe una cadena de bits distinta, $\hat{c}_5$). Al recibir la secuencia de cifrado de 8 bloques, ¿qué bloques del texto claro inicial podrán descifrase correctamente?

*Solución:*

a) El modo CBC no puede paralelizarse, pues para construír el bloque i-ésimo de cifrado $c_i = F_k(m_i \oplus c_{i-1})$ necesitamos el anterior $c_{i-1}$. Sin embargo, el modo CTR puede paralelizarse sin problemas: podemos calcular simultáneamente cada paso, pues el i-ésimo bloque de cifrado $c_i = m_i \oplus F_k(CTR+i)$ no depende de los anteriores.

b) El bloque $c_5$ se altera en la transmisión, es decir, aunque el emisor envía $c_0, c_1, \ldots, c_7$ el receptor recibe $c_0, c_1, c_2, c_4, c_5^*, c_6, c_7$. Recordemos que al descifrar se realiza la operación $m_i := F_k^{-1}(c_i) \oplus c_{i-1}$. Así, a la hora de descifrar el texto $c_5^*$ influye en el descifrado de los bloques 5 y 6, pero todos los demás podrán recuperarse sin problemas.

2. Redes de Feistel: responde a las siguientes preguntas.

   a) Explica la estructura de una red de Feistel y qué herramientas se diseñan típicamente a partir de ellas.

   b) Considera una red de Feistel extructurada en 3 rondas. Actuamos sobre bloques de 16 bits con una clave $K = k_1 \| \cdots \| k_8$ formada por 8 bits, donde todas las funciones de ronda $f_j$ son iguales y se definen como

$$f_j(K, x) = x_1 \oplus k_1 \| x_2 \| x_3 \| x_4 \| x_5 \oplus k_2 \| x_6 \oplus k_7 \| x_7 \| x_8 \oplus k_8.$$

   Cifra el texto claro 0101000011110111. Comenta los fallos de diseño que te parezcan relevantes en la construcción anterior.

*Solución*

a) Teoría. Describir al menos el esquema de cifrado/descifrado subyacente, y subrayar que se utilizan para construir cifradores en bloque.

b) Esquemáticamente, denotemos por $\alpha(k) = (k_1, 0, 0, 0, k_2, k_7, 0, k_8.)$ y es fácil ver que la estructura de la función de ronda es $f_j(K, x) = x \oplus \alpha(k)$. De ese modo, tenemos que en esta red para la ronda i-ésima se construye

$$L_i := R_i \text{ y } R_i := L_{i-1} \oplus R_{i-1} \oplus \alpha(k).$$

Así,

$L_1 = R_0, R_1 = L_0 \oplus R_0 \oplus \alpha(k)$ y por tanto $L_2 = R_1, R_2 = L_1 \oplus L_0 \oplus R_0 = L_0$.

Ahora,

$$L_3 = L_0 \text{ y } R_3 = L_2 \oplus R_2 \oplus \alpha(k) = L_0 \oplus R_0 \oplus \alpha(k) \oplus L_0 \oplus \alpha(k) = R_0.$$

De este modo, de la salida de la red podemos leer directamente el texto claro.

3. Verdadero o falso. Razona tu respuesta.

a. Toda función hash resistente a colisiones (CR) es también resistente a colisiones dirigidas (*target-collision resistant*– (TCR)).

b. Si un problema de decisión está en la clase de complejidad NP, no se conoce ningún algoritmo polinomial para comprobar sus soluciones asociadas.

c. El cifrador en flujo $RC4$ se considera de alta seguridad.

d. Si conocemos la longitud de la clave de un cifrado Vigenere, podemos atacar un texto interceptado a través de un análisis de frecuencias en el alfabeto subyacente.

*Solución:*

a. Verdadero. La seguridad CR implica seguridad TCR; si un adversario no es capaz de crear una colisión arbitraria, tampoco será capaz de crear una dirigida a un reto propuesto.

b. Falso. Por definición, existe un algoritmo polinomial que sirve para comprobar las soluciones asociadas.

c. Falso. Es un cifrador de muy baja seguridad.

d. Verdadero. Si tenemos la longitud de la palabra clave, realizamos ataques a cifrado César por bloques centrados en las posiciones que la palabra determina; dichos ataques serán por análisis de frecuencias.

## Primer Examen Parcial. Modelo B

1.Verdadero o falso. Razona tu respuesta.

a. Toda función hash resistente a colisiones dirigidas (*target-collision resistant*– (TCR)) es también resistente a colisiones (CR).

b. Si conocemos la longitud de la clave de un cifrado Vigenere, podemos atacar un texto interceptado a través de un análisis de frecuencias en el alfabeto subyacente.

c. Si un problema de decisión está en la clase de complejidad NP hard, siempre se conoce un algoritmo polinomial para comprobar sus soluciones asociadas.

d. El cifrador en bloque $AES$ se considera de alta seguridad.

*Solución*

a. Falso. Realizar una colisión dirigida es más dificil que realizar una colisión arbitraria, seguridad TCR no implica seguridad CR (sino al revés).

b. Verdadero. Ver modelo A.

c. Falso, no todos los problemas NP-hard están en la clase NP.

d. Verdadero, visto en clase, es el estándar actual de alta seguridad.

2. Redes de Feistel: responde a las siguientes preguntas.

a) Explica la estructura de una red de Feistel y qué herramientas se diseñan típicamente a partir de ellas.

b) Considera una red de Feistel extructurada en 3 rondas. Actuamos sobre bloques de 16 bits con una clave $K = k_1\| \cdots \|k_8$ formada por 8 bits, donde todas las funciones de ronda $f_j$ son iguales y se definen como

$$f_j(K, x) = x_1 \oplus k_1\|x_2\|x_3\|x_4\|x_5 \oplus k_2\|x_6 \oplus k_7\|x_7 \oplus k_8\|x_8.$$

Cifra el texto claro 0101000011110101. Comenta los fallos de diseño que te parezcan relevantes en la construcción anterior.

*Solución:* Ver modelo A. La red de Feistel es distinta, pero el cifrado resultante es idéntico (no hace nada, puede leerse el texto claro de la salida porque la acción de la clave secreta se cancela).

3. Considera los modos de operación (ECB y CBC) para cifradores en bloque vistos en clase y responde las siguientes preguntas:

a) ¿Cuáles de ellos pueden paralelizarse, es decir, para cuales podemos cifrar $n$ bloques de entrada $m_0, \ldots, m_n$ simultáneamente, y para qué otros hemos de hacerlo necesariamente de modo secuencial (y en el orden prescrito)?

b) Si ciframos un texto $m_1, \ldots, m_7$ con un cifrador en bloque en modo CBC, y se produce un error en la trasmisión del cifrado del bloque $m_5$, (es decir, el emisor construyó $c_5$ pero el receptor recibe una cadena de bits distinta, $c_5^*$). Al recibir la secuencia de cifrado de 8 bloques, ¿qué bloques del texto claro inicial podrán descifrase correctamente?

*Solución:* Ver modelo A. Lo único distinto es que el modo ECB puede, igual que el CTR, paralelizarse sin problemas, por ser el cifrado del bloque i-ésimo $c_i = F_k(m_i)$ independiente de los cifrados de otros bloques.