Aplicaciones de Cuerpos Finitos en la criptografía de clave simétrica

Daniel Penazzi

19 de octubre de 2017

Tabla de Contenidos

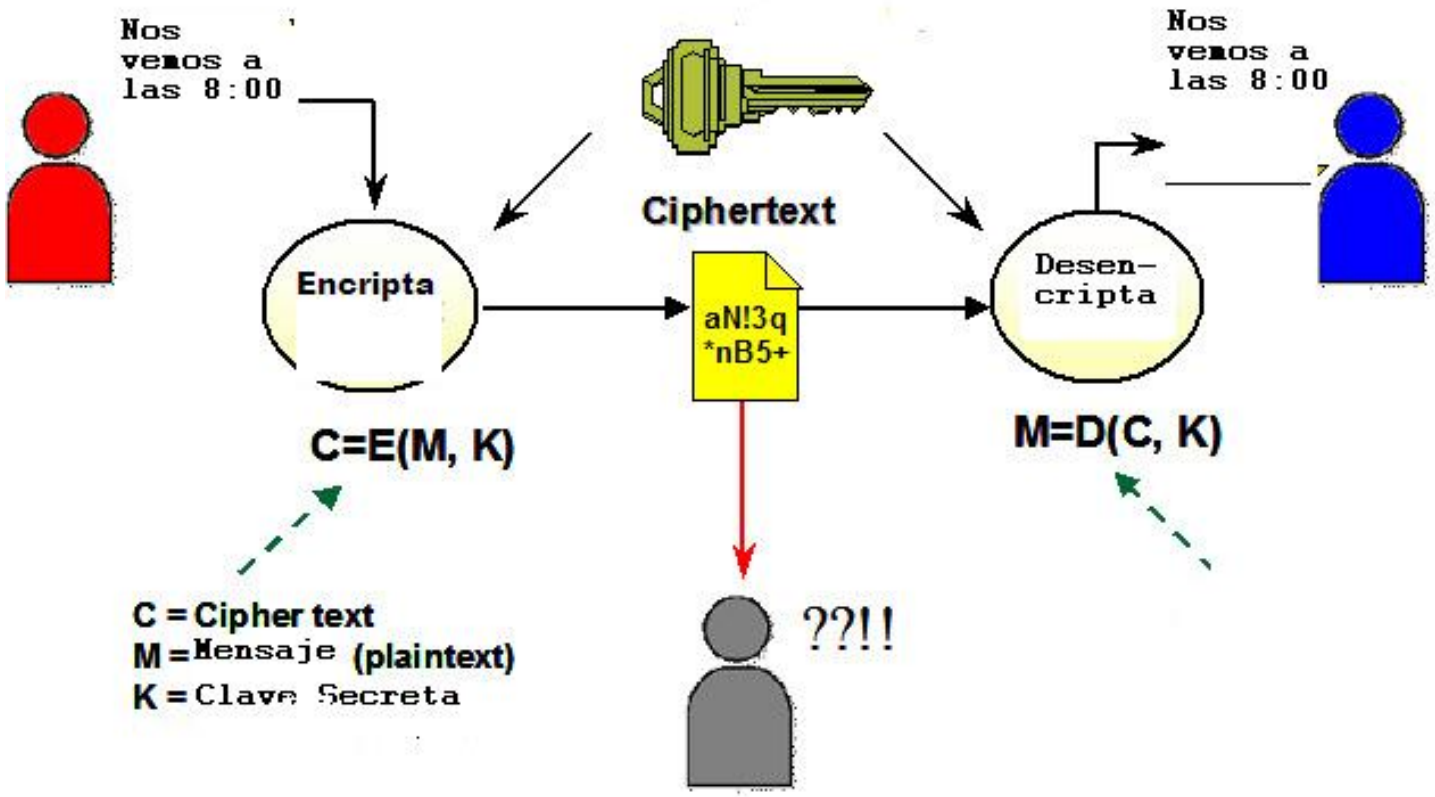
Confidencialidad

- Problema:

Confidencialidad

- Problema:

Solución: Cifradores



Tipos de ataques

- “ciphertext-only”

Tipos de ataques

- “ciphertext-only”
- “known plaintext”.

Tipos de ataques

- “ciphertext-only”
- “known plaintext”.
- “chosen plaintext”.

Tipos de ataques

- “ciphertext-only”
- “known plaintext”.
- “chosen plaintext”.
- “chosen chiphertext”.

Block Ciphers

- Muchos cifradores son del tipo llamado block cipher (cifradores de bloque) o cifradores de substitución.

Block Ciphers

- Muchos cifradores son del tipo llamado block cipher (cifradores de bloque) o cifradores de substitución.
- $m = m_1||m_2||...$

Block Ciphers

- Muchos cifradores son del tipo llamado block cipher (cifradores de bloque) o cifradores de substitución.
- $m = m_1||m_2||...$
- ECB: $c_i = E_K(m_i)$

Block Ciphers

- Muchos cifradores son del tipo llamado block cipher (cifradores de bloque) o cifradores de substitución.
- $m = m_1||m_2||...$
- ECB: $c_i = E_K(m_i)$
  - $m_i = m_j \Rightarrow c_i = c_j$

Block Ciphers

- Muchos cifradores son del tipo llamado block cipher (cifradores de bloque) o cifradores de substitución.
- $m = m_1||m_2||...$
- ECB: $c_i = E_K(m_i)$
  - $m_i = m_j \Rightarrow c_i = c_j$
- CBC: $c_i = E_k(m_i \oplus c_{i-1})$. $(c_0 = IV)$

Block Ciphers

- Muchos cifradores son del tipo llamado block cipher (cifradores de bloque) o cifradores de substitución.
- $m = m_1||m_2||...$
- ECB: $c_i = E_K(m_i)$
  - $m_i = m_j \Rightarrow c_i = c_j$
- CBC: $c_i = E_k(m_i \oplus c_{i-1})$. $(c_0 = IV)$
- Counter $c_i = m_i \oplus E_k(IV + i)$

ECB - Electronic Codebook

Patrones en el texto cifrado. (imagen de M.Montes)

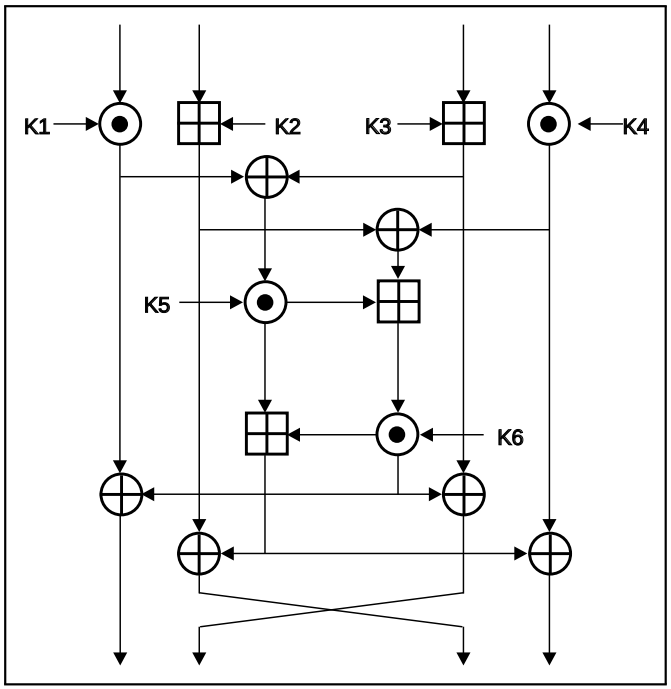


Imagen original

ECB - Electronic Codebook

Patrones en el texto cifrado. (imagen de M.Montes)

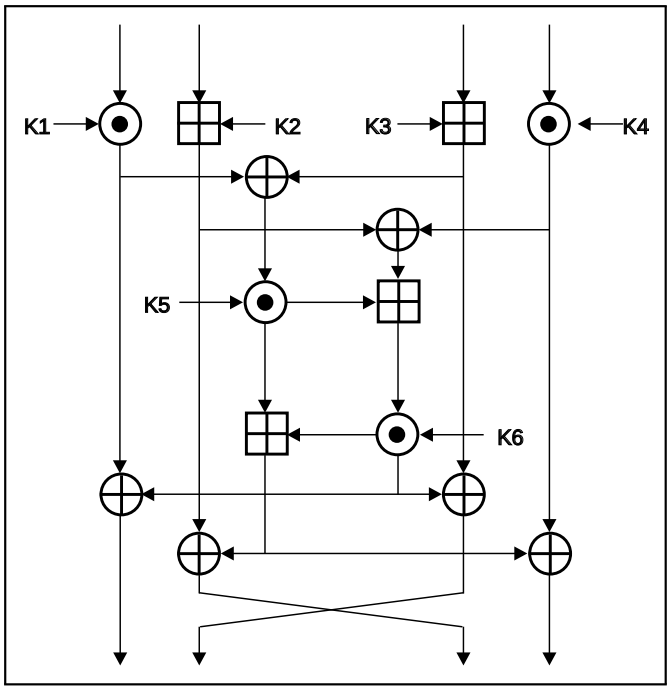
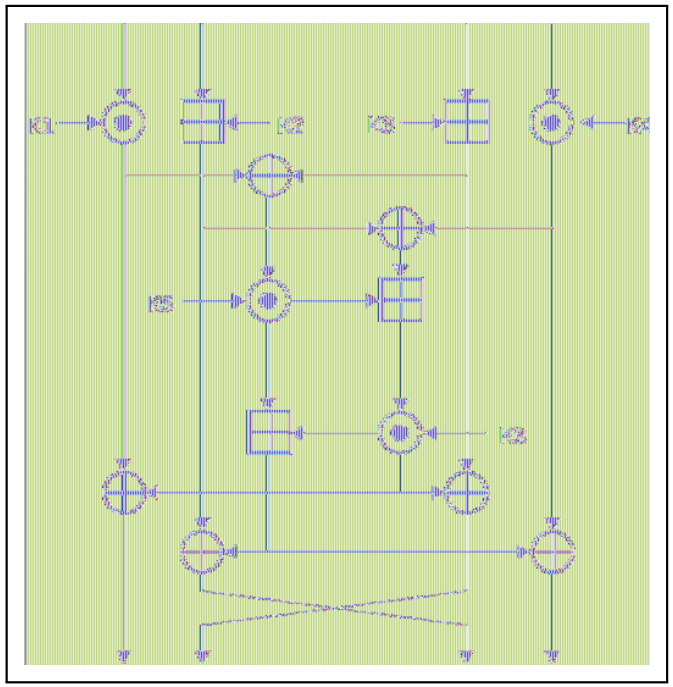


Imagen original



Cifrada en modo ECB

Rondas

- Bloques demasiado chicos permiten diversos ataques.

Rondas

- Bloques demasiado chicos permiten diversos ataques.
- En la actualidad los cifradores de bloque mas usados tienen tamaño de 128 bits.

Rondas

- Bloques demasiado chicos permiten diversos ataques.
- En la actualidad los cifradores de bloque mas usados tienen tamaño de 128 bits.
- No se puede hacer una tabla con 2^{128} entradas.

Rondas

- Bloques demasiado chicos permiten diversos ataques.
- En la actualidad los cifradores de bloque mas usados tienen tamaño de 128 bits.
- No se puede hacer una tabla con 2^{128} entradas.
- ¿cómo implementar un cifrador con un bloque tan grande?

Rondas

- Bloques demasiado chicos permiten diversos ataques.
- En la actualidad los cifradores de bloque mas usados tienen tamaño de 128 bits.
- No se puede hacer una tabla con 2^{128} entradas.
- ¿cómo implementar un cifrador con un bloque tan grande?
- Se pueden usar operaciones sobre subbloques mas chicos.

Rondas

- Bloques demasiado chicos permiten diversos ataques.
- En la actualidad los cifradores de bloque mas usados tienen tamaño de 128 bits.
- No se puede hacer una tabla con 2^{128} entradas.
- ¿cómo implementar un cifrador con un bloque tan grande?
- Se pueden usar operaciones sobre subbloques mas chicos.
- Pero hay que asegurarse que todos los bits de la salida dependan de todos los bits de la entrada.

Rondas

- Bloques demasiado chicos permiten diversos ataques.
- En la actualidad los cifradores de bloque mas usados tienen tamaño de 128 bits.
- No se puede hacer una tabla con 2^{128} entradas.
- ¿cómo implementar un cifrador con un bloque tan grande?
- Se pueden usar operaciones sobre subbloques mas chicos.
- Pero hay que asegurarse que todos los bits de la salida dependan de todos los bits de la entrada.
- Una técnica básica de los cifradores modernos es repetir sus operaciones a lo largo de varias "rondas".

Rondas

- Bloques demasiado chicos permiten diversos ataques.
- En la actualidad los cifradores de bloque mas usados tienen tamaño de 128 bits.
- No se puede hacer una tabla con 2^{128} entradas.
- ¿cómo implementar un cifrador con un bloque tan grande?
- Se pueden usar operaciones sobre subbloques mas chicos.
- Pero hay que asegurarse que todos los bits de la salida dependan de todos los bits de la entrada.
- Una técnica básica de los cifradores modernos es repetir sus operaciones a lo largo de varias "rondas".
- Ejemplo: DES: 16 rondas, AES 10,12 o 14 rondas, etc.

Cifradores de Hill

- En la decada del 1920 Hill inventó cifradores con bloques relativamente grandes para la epoca usando transformaciones lineales sobre $\mathbb{Z}_n$, de forma tal que todos las letras de salida dependieran de todas las letras de entrada.

Cifradores de Hill

- En la decada del 1920 Hill inventó cifradores con bloques relativamente grandes para la epoca usando transformaciones lineales sobre $\mathbb{Z}_n$, de forma tal que todos las letras de salida dependieran de todas las letras de entrada.
- Los cifradores de Hill son resistentes a ataques de tipo ciphertext only, pero son muy débiles contra ataques de tipo chosen plaintext.

Cifradores de Hill

- En la decada del 1920 Hill inventó cifradores con bloques relativamente grandes para la epoca usando transformaciones lineales sobre $\mathbb{Z}_n$, de forma tal que todos las letras de salida dependieran de todas las letras de entrada.
- Los cifradores de Hill son resistentes a ataques de tipo ciphertext only, pero son muy débiles contra ataques de tipo chosen plaintext.
  - Basta un numero relativamente bajo de textos planos linealmente independientes para quebrarlo

Cifradores de Hill

- En la decada del 1920 Hill inventó cifradores con bloques relativamente grandes para la epoca usando transformaciones lineales sobre $\mathbb{Z}_n$, de forma tal que todos las letras de salida dependieran de todas las letras de entrada.
- Los cifradores de Hill son resistentes a ataques de tipo ciphertext only, pero son muy débiles contra ataques de tipo chosen plaintext.
  - Basta un numero relativamente bajo de textos planos linealmente independientes para quebrarlo
- La lección aprendida con Hill es que todos los cifradores deben tener al menos una componente no lineal.

Técnicas de construcción de cifradores

- Una técnica es usar operaciones matemáticas o lógicas que no sean compatibles entre sí . (es decir, que no sean todas lineales respecto del mismo espacio vectorial)

Técnicas de construcción de cifradores

- Una técnica es usar operaciones matemáticas o lógicas que no sean compatibles entre sí . (es decir, que no sean todas lineales respecto del mismo espacio vectorial)
- Hay varios algoritmos que usan una mezcla de operaciones no compatibles entre si.

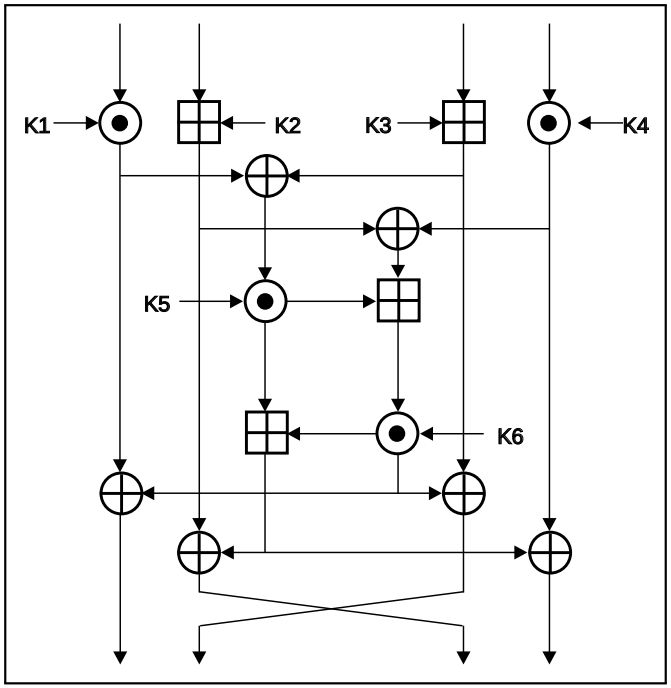
Técnicas de construcción de cifradores

- Una técnica es usar operaciones matemáticas o lógicas que no sean compatibles entre sí . (es decir, que no sean todas lineales respecto del mismo espacio vectorial)
- Hay varios algoritmos que usan una mezcla de operaciones no compatibles entre si.
- Por ejemplo, el cifrador RC6 de 128 bits, mira el estado interno como cuatro registros de 32 bits, y usa XOR bit a bit, sumas y multiplicaciones modulo 2^{32}, rotaciones de 5 bits, y 32-bit Data Dependent Rotations. (un registro se rota de acuerdo a lo que esta guardado en otro registro).

Técnicas de construcción de cifradores

- Una técnica es usar operaciones matemáticas o lógicas que no sean compatibles entre sí . (es decir, que no sean todas lineales respecto del mismo espacio vectorial)
- Hay varios algoritmos que usan una mezcla de operaciones no compatibles entre si.
- Por ejemplo, el cifrador RC6 de 128 bits, mira el estado interno como cuatro registros de 32 bits, y usa XOR bit a bit, sumas y multiplicaciones modulo 2^{32}, rotaciones de 5 bits, y 32-bit Data Dependent Rotations. (un registro se rota de acuerdo a lo que esta guardado en otro registro).
- Otro cifrador famoso es IDEA, de 64 bits, que usaba sumas modulo 2^{16}, XORs bits a bits, y multiplicaciones en $\mathbb{Z}_{2^{16}+1} - \{0\}$.

Una ronda de IDEA



Problemas con este tipo de cifradores

- Un problema con este tipo de cifradores es que sufren una penalidad de implementación en arquitecturas no nativas al diseño, particularmente en arquitecturas orientadas a bytes.

Problemas con este tipo de cifradores

- Un problema con este tipo de cifradores es que sufren una penalidad de implementación en arquitecturas no nativas al diseño, particularmente en arquitecturas orientadas a bytes.
- Y las rotaciones, si son rotaciones de registros de 32 bits, sufren una penalidad en entornos de 64 bits, y viceversa

Problemas con este tipo de cifradores

- Un problema con este tipo de cifradores es que sufren una penalidad de implementación en arquitecturas no nativas al diseño, particularmente en arquitecturas orientadas a bytes.
- Y las rotaciones, si son rotaciones de registros de 32 bits, sufren una penalidad en entornos de 64 bits, y viceversa
- Ademas, es bastante difícil analizarlos y poder obtener cotas de seguridad demonstrables.

Problemas con este tipo de cifradores

- Un problema con este tipo de cifradores es que sufren una penalidad de implementación en arquitecturas no nativas al diseño, particularmente en arquitecturas orientadas a bytes.
- Y las rotaciones, si son rotaciones de registros de 32 bits, sufren una penalidad en entornos de 64 bits, y viceversa
- Ademas, es bastante difícil analizarlos y poder obtener cotas de seguridad demonstrables.
- El estandard actual (AES) y el anterior (DES) no son de ese tipo sin embargo sino que usan otro tipo de ideas para poder operar sobre bloques grandes.

Combinando cosas

- AES y DES lo que hacen es combinar, en cada ronda:

Combinando cosas

- AES y DES lo que hacen es combinar, en cada ronda:
  - substituciones no lineales chicas (para que sean eficientes) ("S-boxes")

Combinando cosas

- AES y DES lo que hacen es combinar, en cada ronda:
  - substituciones no lineales chicas (para que sean eficientes) ("S-boxes")
  - con transformaciones lineales del bloque.

Combinando cosas

- AES y DES lo que hacen es combinar, en cada ronda:
  - substituciones no lineales chicas (para que sean eficientes) ("S-boxes")
  - con transformaciones lineales del bloque.
- Los Sboxes se analizan exhaustivamente para lograr resistencia a ataques de aproximaciones lineales, y la transformación lineal se encarga de “difundir" los cambios locales efectuados por el Sbox a todo el bloque, a lo largo de varias rondas.

AES

- La clave se “expande" para obtener todas las claves de ronda necesarias:

AES

- La clave se “expande" para obtener todas las claves de ronda necesarias:
  - 128 de esos bits expandidos se usan para hacer XOR con el bloque al principio de toda la operación.

AES

- La clave se “expande" para obtener todas las claves de ronda necesarias:
  - 128 de esos bits expandidos se usan para hacer XOR con el bloque al principio de toda la operación.
  - Las otras secuencias generadas de 128 bits se xorean con el bloque al final de cada ronda.

AES

- La clave se “expande" para obtener todas las claves de ronda necesarias:
  - 128 de esos bits expandidos se usan para hacer XOR con el bloque al principio de toda la operación.
  - Las otras secuencias generadas de 128 bits se xorean con el bloque al final de cada ronda.
- Cada ronda tiene, ademas de ese xor final, otras tres partes:

AES

- La clave se “expande" para obtener todas las claves de ronda necesarias:
  - 128 de esos bits expandidos se usan para hacer XOR con el bloque al principio de toda la operación.
  - Las otras secuencias generadas de 128 bits se xorean con el bloque al final de cada ronda.
- Cada ronda tiene, ademas de ese xor final, otras tres partes:
  1. Una substitución de bytes por bytes

AES

- La clave se “expande" para obtener todas las claves de ronda necesarias:
  - 128 de esos bits expandidos se usan para hacer XOR con el bloque al principio de toda la operación.
  - Las otras secuencias generadas de 128 bits se xorean con el bloque al final de cada ronda.
- Cada ronda tiene, ademas de ese xor final, otras tres partes:
  1. Una substitución de bytes por bytes
  2. Una transformación lineal de los 16 bytes compuesta de dos partes:

AES

- La clave se “expande" para obtener todas las claves de ronda necesarias:
  - 128 de esos bits expandidos se usan para hacer XOR con el bloque al principio de toda la operación.
  - Las otras secuencias generadas de 128 bits se xorean con el bloque al final de cada ronda.
- Cada ronda tiene, ademas de ese xor final, otras tres partes:
  1. Una substitución de bytes por bytes
  2. Una transformación lineal de los 16 bytes compuesta de dos partes:
     1. Un cambio de lugares de bytes en el arreglo de bytes que componen el bloque

AES

- La clave se “expande" para obtener todas las claves de ronda necesarias:
  - 128 de esos bits expandidos se usan para hacer XOR con el bloque al principio de toda la operación.
  - Las otras secuencias generadas de 128 bits se xorean con el bloque al final de cada ronda.
- Cada ronda tiene, ademas de ese xor final, otras tres partes:
  1. Una substitución de bytes por bytes
  2. Una transformación lineal de los 16 bytes compuesta de dos partes:
     1. Un cambio de lugares de bytes en el arreglo de bytes que componen el bloque
     2. Una transformación lineal de subconjuntos de 4 bytes en subconjuntos de 4 bytes, dada por una multiplicación por una matriz 4×4 de bytes. (no se hace en la ultima ronda)

Cuerpos Finitos

- Cuando hablamos de una matriz de bytes, que multiplica bytes, ¿de que operaciónes de suma y producto estamos hablando?

Cuerpos Finitos

- Cuando hablamos de una matriz de bytes, que multiplica bytes, ¿de que operaciónes de suma y producto estamos hablando?
- Una posibilidad podría ser usar suma y producto módulo 2^8, pero $\mathbb{Z}_{2^8}$ no es un cuerpo y los diseñadores de Rijndael necesitaban un cuerpo para poder probar ciertas propiedades del cifrador que querían que este tuviera.

Cuerpos Finitos

- Cuando hablamos de una matriz de bytes, que multiplica bytes, ¿de que operaciónes de suma y producto estamos hablando?
- Una posibilidad podría ser usar suma y producto módulo 2^8, pero $\mathbb{Z}_{2^8}$ no es un cuerpo y los diseñadores de Rijndael necesitaban un cuerpo para poder probar ciertas propiedades del cifrador que querían que este tuviera.
- En Cripto se suelen usar los cuerpos finitos de la forma $GF(2^n)$ para algún n. Rijndael usa $GF(2^8)$ para hacer sus operaciones.

Cuerpos Finitos

- Cuando hablamos de una matriz de bytes, que multiplica bytes, ¿de que operaciónes de suma y producto estamos hablando?
- Una posibilidad podría ser usar suma y producto módulo 2^8, pero $\mathbb{Z}_{2^8}$ no es un cuerpo y los diseñadores de Rijndael necesitaban un cuerpo para poder probar ciertas propiedades del cifrador que querían que este tuviera.
- En Cripto se suelen usar los cuerpos finitos de la forma $GF(2^n)$ para algún n. Rijndael usa $GF(2^8)$ para hacer sus operaciones.
- ¿Porqué necesitan un cuerpo? Para obtener resistencia contra dos tipos de ataques muy poderosos: el criptoanálisis diferencial y el criptoanálisis lineal.

DC

- En el Criptoanálisis Diferencial se tratan de explotar las desviaciones estadísticas entre las **diferencias** de los datos de entrada y los datos de salida de alguna componente no lineal (Sboxes, operacion aritmética no lineal, etc).

DC

- En el Criptoanálisis Diferencial se tratan de explotar las desviaciones estadísticas entre las **diferencias** de los datos de entrada y los datos de salida de alguna componente no lineal (Sboxes, operacion aritmética no lineal, etc).
- “diferencia" es relativa a algún grupo.

DC

- En el Criptoanálisis Diferencial se tratan de explotar las desviaciones estadísticas entre las **diferencias** de los datos de entrada y los datos de salida de alguna componente no lineal (Sboxes, operacion aritmética no lineal, etc).
- “diferencia" es relativa a algún grupo. En general, $\mathbb{Z}_2^n$, pero dependiendo del cifrador puede ser mas conveniente usar otros grupos.

DC

- En el Criptoanálisis Diferencial se tratan de explotar las desviaciones estadísticas entre las **diferencias** de los datos de entrada y los datos de salida de alguna componente no lineal (Sboxes, operacion aritmética no lineal, etc).
- “diferencia" es relativa a algún grupo. En general, $\mathbb{Z}_2^n$, pero dependiendo del cifrador puede ser mas conveniente usar otros grupos. Básicamente, se debe usar el grupo que el cifrador usa para mesclar las claves de ronda con el texto.

DC

- Denotemos la suma de $\mathbb{Z}_2^n$ por $\oplus$.

DC

- Denotemos la suma de $\mathbb{Z}_2^n$ por $\oplus$.
- Dados $R, R' \in \mathbb{Z}_2^n$, denotemos $\Delta_R = R \oplus R'$.

DC

- Denotemos la suma de $\mathbb{Z}_2^n$ por $\oplus$.
- Dados $R, R' \in \mathbb{Z}_2^n$, denotemos $\Delta_R = R \oplus R'$. (si el grupo en cuestión no es $\mathbb{Z}_2^n$ se tomaría la diferencia del grupo en vez de $\oplus$).

DC

- Denotemos la suma de $\mathbb{Z}_2^n$ por $\oplus$.
- Dados $R, R' \in \mathbb{Z}_2^n$, denotemos $\Delta_R = R \oplus R'$. (si el grupo en cuestión no es $\mathbb{Z}_2^n$ se tomaría la diferencia del grupo en vez de $\oplus$).
- Si P, P' denota dos textos planos y C, C' sus textos cifrados correspondientes, en el random cipher no habrá ninguna relación predecible entre Δ_P y Δ_C.

DC

- Denotemos la suma de $\mathbb{Z}_2^n$ por $\oplus$.
- Dados $R, R' \in \mathbb{Z}_2^n$, denotemos $\Delta_R = R \oplus R'$. (si el grupo en cuestión no es $\mathbb{Z}_2^n$ se tomaría la diferencia del grupo en vez de $\oplus$).
- Si P, P' denota dos textos planos y C, C' sus textos cifrados correspondientes, en el random cipher no habrá ninguna relación predecible entre Δ_P y Δ_C.
- Si se encuentra alguna relación entre ellos en un cifrador real, esto constituye un ataque de distinguibilidad.

- Por ejemplo, consideremos una ronda del tipo:

- Por ejemplo, consideremos una ronda del tipo:
-

$$P \xrightarrow{\oplus k} X \xrightarrow{Sbox} Y \xrightarrow{tr.lineal} Z \xrightarrow{\oplus k^*} C$$

- Por ejemplo, consideremos una ronda del tipo:
- $$P \xrightarrow{\oplus k} X \xrightarrow{Sbox} Y \xrightarrow{tr.lineal} Z \xrightarrow{\oplus k^*} C$$
- Sbox y tr.lineal se suponen conocidos, k y k^* son los secretos.

- Por ejemplo, consideremos una ronda del tipo:
- $$P \xrightarrow{\oplus k} X \xrightarrow{Sbox} Y \xrightarrow{tr.lineal} Z \xrightarrow{\oplus k^*} C$$
- Sbox y tr.lineal se suponen conocidos, k y k^* son los secretos.
- Dados textos planos P y P' denotemos por X, X', Y, Y', etc sus evoluciones a lo largo del cifrador.

- Por ejemplo, consideremos una ronda del tipo:
- $$P \xrightarrow{\oplus k} X \xrightarrow{Sbox} Y \xrightarrow{tr.lineal} Z \xrightarrow{\oplus k^*} C$$
- Sbox y tr.lineal se suponen conocidos, k y k^* son los secretos.
- Dados textos planos P y P' denotemos por X, X', Y, Y', etc sus evoluciones a lo largo del cifrador.
- Queremos ver como evolucionan Δ_X, Δ_Y, etc, teniendo en cuenta que el adversario no conoce las claves.

- Por ejemplo, consideremos una ronda del tipo:
- $$P \xrightarrow{\oplus k} X \xrightarrow{Sbox} Y \xrightarrow{tr.lineal} Z \xrightarrow{\oplus k^*} C$$
- Sbox y tr.lineal se suponen conocidos, k y k^* son los secretos.
- Dados textos planos P y P' denotemos por X, X', Y, Y', etc sus evoluciones a lo largo del cifrador.
- Queremos ver como evolucionan Δ_X, Δ_Y, etc, teniendo en cuenta que el adversario no conoce las claves.

$$\Delta_X = X \oplus X'$$

- Por ejemplo, consideremos una ronda del tipo:
- $$P \xrightarrow{\oplus k} X \xrightarrow{Sbox} Y \xrightarrow{tr.lineal} Z \xrightarrow{\oplus k^*} C$$
- Sbox y tr.lineal se suponen conocidos, k y k^* son los secretos.
- Dados textos planos P y P' denotemos por X, X', Y, Y', etc sus evoluciones a lo largo del cifrador.
- Queremos ver como evolucionan Δ_X, Δ_Y, etc, teniendo en cuenta que el adversario no conoce las claves.

$$\Delta_X = X \oplus X' = (P \oplus k) \oplus (P' \oplus k)$$

- Por ejemplo, consideremos una ronda del tipo:
- $$P \xrightarrow{\oplus k} X \xrightarrow{Sbox} Y \xrightarrow{tr.lineal} Z \xrightarrow{\oplus k^*} C$$
- Sbox y tr.lineal se suponen conocidos, k y k^* son los secretos.
- Dados textos planos P y P' denotemos por X, X', Y, Y', etc sus evoluciones a lo largo del cifrador.
- Queremos ver como evolucionan Δ_X, Δ_Y, etc, teniendo en cuenta que el adversario no conoce las claves.

$$\Delta_X = X \oplus X' = (P \oplus k) \oplus (P' \oplus k) = P \oplus P'$$

- Por ejemplo, consideremos una ronda del tipo:
- $$P \xrightarrow{\oplus k} X \xrightarrow{Sbox} Y \xrightarrow{tr.lineal} Z \xrightarrow{\oplus k^*} C$$
- Sbox y tr.lineal se suponen conocidos, k y k^* son los secretos.
- Dados textos planos P y P' denotemos por X, X', Y, Y', etc sus evoluciones a lo largo del cifrador.
- Queremos ver como evolucionan Δ_X, Δ_Y, etc, teniendo en cuenta que el adversario no conoce las claves.

$$\begin{aligned} \Delta_X &= X \oplus X' = (P \oplus k) \oplus (P' \oplus k) = P \oplus P' \\ &= \Delta_P \end{aligned}$$

Bypassing la clave

- De la misma forma, $\Delta_C = \Delta_Z$.

Bypassing la clave

- De la misma forma, $\Delta_C = \Delta_Z$.
- Ademas, $\Delta_Z = tr.lineal(\Delta_Y)$.

Bypassing la clave

- De la misma forma, $\Delta_C = \Delta_Z$.
- Ademas, $\Delta_Z = tr.lineal(\Delta_Y)$.
- Estas relaciónes son verdaderas independientemente de k y de quienes son P, P', X, X', etc (sólo dependen de los Δ's).

Bypassing la clave

- De la misma forma, $\Delta_C = \Delta_Z$.
- Ademas, $\Delta_Z = tr.lineal(\Delta_Y)$.
- Estas relaciónes son verdaderas independientemente de k y de quienes son P, P', X, X', etc (sólo dependen de los Δ's).
- El problema es cúal es la relación entre Δ_X y Δ_Y.

Bypassing la clave

- De la misma forma, $\Delta_C = \Delta_Z$.
- Ademas, $\Delta_Z = tr.lineal(\Delta_Y)$.
- Estas relaciónes son verdaderas independientemente de k y de quienes son P, P', X, X', etc (sólo dependen de los Δ's).
- El problema es cúal es la relación entre Δ_X y Δ_Y.
- $\nexists f$ tal que $\Delta_Y = f(\Delta_X)$ debido a la no linealidad del S-box.

Bypassing la clave

- De la misma forma, $\Delta_C = \Delta_Z$.
- Ademas, $\Delta_Z = tr.lineal(\Delta_Y)$.
- Estas relaciónes son verdaderas independientemente de k y de quienes son P, P', X, X', etc (sólo dependen de los Δ's).
- El problema es cúal es la relación entre Δ_X y Δ_Y.
- $\nexists f$ tal que $\Delta_Y = f(\Delta_X)$ debido a la no linealidad del S-box.
- Sin embargo, el nucleo del DC es lo siguiente:

Bypassing la clave

- De la misma forma, $\Delta_C = \Delta_Z$.
- Ademas, $\Delta_Z = tr.lineal(\Delta_Y)$.
- Estas relaciónes son verdaderas independientemente de k y de quienes son P, P', X, X', etc (sólo dependen de los Δ's).
- El problema es cúal es la relación entre Δ_X y Δ_Y.
- $\nexists f$ tal que $\Delta_Y = f(\Delta_X)$ debido a la no linealidad del S-box.
- Sin embargo, el nucleo del DC es lo siguiente:

Importante!

Dado un Δ_X no todo Δ_Y es igualmente probable.

- Si Δ_X queda fijo entonces X determina Δ_Y:

- Si Δ_X queda fijo entonces X determina Δ_Y:

$$\Delta_Y \quad = \quad Y \oplus Y'$$

- Si Δ_X queda fijo entonces X determina Δ_Y:

$$\begin{aligned} \Delta_Y &= Y \oplus Y' \\ &= S(X) \oplus S(X') \end{aligned}$$

- Si Δ_X queda fijo entonces X determina Δ_Y:

$$\begin{aligned} \Delta_Y &= Y \oplus Y' \\ &= S(X) \oplus S(X') \\ &= S(X) \oplus S(X \oplus \Delta_X) \end{aligned}$$

- Si Δ_X queda fijo entonces X determina Δ_Y:

$$\begin{aligned} \Delta_Y &= Y \oplus Y' \\ &= S(X) \oplus S(X') \\ &= S(X) \oplus S(X \oplus \Delta_X) \end{aligned}$$

- Pero el atacante NO CONOCE X, que en general depende de la clave.

- Si Δ_X queda fijo entonces X determina Δ_Y:

$$\begin{aligned} \Delta_Y &= Y \oplus Y' \\ &= S(X) \oplus S(X') \\ &= S(X) \oplus S(X \oplus \Delta_X) \end{aligned}$$

- Pero el atacante NO CONOCE X, que en general depende de la clave.
- Asi que deberá calcular probabilidades sobre X, de que un dado Δ_X se transforme en un Δ_Y.

$\Delta_X = 3$

- Veamos un ejemplo para $n = 3$.

$\Delta_X = 3$

- Veamos un ejemplo para $n = 3$.
- Denotaremos $001 = 1$, $010 = 2$, $011 = 3$, etc.

$\Delta_X = 3$

- Veamos un ejemplo para $n = 3$.
- Denotaremos $001 = 1$, $010 = 2$, $011 = 3$, etc.
- Tomaremos $S = 34567012$, es decir, $S(0) = 3$, $S(1) = 4$, etc.

$\Delta_X = 3$

- Veamos un ejemplo para $n = 3$.
- Denotaremos $001 = 1$, $010 = 2$, $011 = 3$, etc.
- Tomaremos $S = 34567012$, es decir, $S(0) = 3$, $S(1) = 4$, etc.
- Supongamos que $\Delta_X = 3 = 011$. Analicemos los posibles Δ_Y:

$\Delta_X = 3$

- Veamos un ejemplo para $n = 3$.
- Denotaremos $001 = 1$, $010 = 2$, $011 = 3$, etc.
- Tomaremos $S = 34567012$, es decir, $S(0) = 3$, $S(1) = 4$, etc.
- Supongamos que $\Delta_X = 3 = 011$. Analicemos los posibles Δ_Y:

$$\begin{array}{rlrl} X: & 01234567 & Y = S(X): & 34567012 \\ X' = X \oplus \Delta_X: & 32107654 & Y' = S(X'): & 65432107 \end{array}$$

$\Delta_X = 3$

- Veamos un ejemplo para $n = 3$.
- Denotaremos $001 = 1$, $010 = 2$, $011 = 3$, etc.
- Tomaremos $S = 34567012$, es decir, $S(0) = 3$, $S(1) = 4$, etc.
- Supongamos que $\Delta_X = 3 = 011$. Analicemos los posibles Δ_Y:

$$\begin{array}{rlrl} X: & 01234567 & Y = S(X): & 34567012 \\ X' = X \oplus \Delta_X: & 32107654 & Y' = S(X'): & 65432107 \\ & & \Delta_Y: & 51155115 \end{array}$$

Probabilidad condicional

- Unicos valores posibles para Δ_Y con ese Δ_X son 1 o 5, ambos la mitad de las veces.

Probabilidad condicional

- Unicos valores posibles para Δ_Y con ese Δ_X son 1 o 5, ambos la mitad de las veces.
- X depende de la primera clave, que no conocemos.

Probabilidad condicional

- Unicos valores posibles para Δ_Y con ese Δ_X son 1 o 5, ambos la mitad de las veces.
- X depende de la primera clave, que no conocemos.
- Tomando probabilidad respecto de ella:

Probabilidad condicional

- Unicos valores posibles para Δ_Y con ese Δ_X son 1 o 5, ambos la mitad de las veces.
- X depende de la primera clave, que no conocemos.
- Tomando probabilidad respecto de ella:
- $P(\Delta_Y = \beta | \Delta_X = 3) = \begin{cases} 0 & si\ \beta \neq 1,5 \\ \frac{4}{8} = 50\% & si\ \beta = 1,5 \end{cases}$

Probabilidad condicional

- Unicos valores posibles para Δ_Y con ese Δ_X son 1 o 5, ambos la mitad de las veces.
- X depende de la primera clave, que no conocemos.
- Tomando probabilidad respecto de ella:
- $P(\Delta_Y = \beta | \Delta_X = 3) = \begin{cases} 0 & si\ \beta \neq 1,5 \\ \frac{4}{8} = 50\% & si\ \beta = 1,5 \end{cases}$
- Por lo tanto, si bien no podemos predecir con exactitud cual será Δ_Y, podemos estimarlo, con cierta probabilidad.

DP

Definition

La probabilidad diferencial es:

DP

Definition

La probabilidad diferencial es:

$$DP(\alpha, \beta) \quad = \quad DP(\alpha \mapsto \beta) = P(\Delta_Y = \beta | \Delta_X = \alpha)$$

DP

Definition

La probabilidad diferencial es:

$$\begin{aligned} DP(\alpha, \beta) &= DP(\alpha \mapsto \beta) = P(\Delta_Y = \beta | \Delta_X = \alpha) \\ &= \frac{\#\{x \in \mathbb{Z}_2^n : S(x) \oplus S(x \oplus \alpha) = \beta\}}{2^n} \end{aligned}$$

DP

Definition

La probabilidad diferencial es:

$$\begin{aligned} DP(\alpha,\beta) &= DP(\alpha \mapsto \beta) = P(\Delta_Y = \beta | \Delta_X = \alpha) \\ &= \frac{\#\{x \in \mathbb{Z}_2^n : S(x) \oplus S(x \oplus \alpha) = \beta\}}{2^n} \end{aligned}$$

Se puede construir la tabla de probabilidades, o bien la tabla de distribución de diferencias, que es la misma pero multiplicada por 2^n.

DP

Definition

La probabilidad diferencial es:

$$\begin{aligned} DP(\alpha,\beta) &= DP(\alpha \mapsto \beta) = P(\Delta_Y = \beta | \Delta_X = \alpha) \\ &= \frac{\#\{x \in \mathbb{Z}_2^n : S(x) \oplus S(x \oplus \alpha) = \beta\}}{2^n} \end{aligned}$$

Se puede construir la tabla de probabilidades, o bien la tabla de distribución de diferencias, que es la misma pero multiplicada por 2^n. Puesto que $DP(0,\beta) = 0$ si $\beta \neq 0$

DP

Definition

La probabilidad diferencial es:

$$\begin{aligned} DP(\alpha,\beta) &= DP(\alpha \mapsto \beta) = P(\Delta_Y = \beta | \Delta_X = \alpha) \\ &= \frac{\#\{x \in \mathbb{Z}_2^n : S(x) \oplus S(x \oplus \alpha) = \beta\}}{2^n} \end{aligned}$$

Se puede construir la tabla de probabilidades, o bien la tabla de distribución de diferencias, que es la misma pero multiplicada por 2^n. Puesto que $DP(0,\beta) = 0$ si $\beta \neq 0$, $DP(0,0) = 1$

DP

Definition

La probabilidad diferencial es:

$$\begin{aligned} DP(\alpha,\beta) &= DP(\alpha \mapsto \beta) = P(\Delta_Y = \beta | \Delta_X = \alpha) \\ &= \frac{\#\{x \in \mathbb{Z}_2^n : S(x) \oplus S(x \oplus \alpha) = \beta\}}{2^n} \end{aligned}$$

Se puede construir la tabla de probabilidades, o bien la tabla de distribución de diferencias, que es la misma pero multiplicada por 2^n. Puesto que $DP(0,\beta) = 0$ si $\beta \neq 0$, $DP(0,0) = 1$y si S es biyeccion, $DP(\alpha,0) = 0$ si $\alpha \neq 0$

DP

Definition

La probabilidad diferencial es:

$$\begin{aligned} DP(\alpha,\beta) &= DP(\alpha \mapsto \beta) = P(\Delta_Y = \beta | \Delta_X = \alpha) \\ &= \frac{\#\{x \in \mathbb{Z}_2^n : S(x) \oplus S(x \oplus \alpha) = \beta\}}{2^n} \end{aligned}$$

Se puede construir la tabla de probabilidades, o bien la tabla de distribución de diferencias, que es la misma pero multiplicada por 2^n. Puesto que $DP(0,\beta) = 0$ si $\beta \neq 0$, $DP(0,0) = 1$y si S es biyeccion, $DP(\alpha,0) = 0$ si $\alpha \neq 0$ en la tabla se suelen eliminar la primera fila y columnas por ser triviales si el Sbox es biyectivo.

tabla para $S = 34567012$

	1	2	3	4	5	6	7
1	0	0	4	0	0	0	4
2	0	4	0	0	0	4	0
3	4	0	0	0	4	0	0
4	0	0	0	8	0	0	0
5	0	0	4	0	0	0	4
6	0	4	0	0	0	4	0
7	4	0	0	0	4	0	0

δ-uniformidad

Una permutación $S : \mathbb{Z}_2^n \mapsto \mathbb{Z}_2^n$ se dice δ-uniforme si:

δ-uniformidad

Una permutación $S : \mathbb{Z}_2^n \mapsto \mathbb{Z}_2^n$ se dice δ-uniforme si:

$$\#\{x \in \mathbb{Z}_2^n : S(x) \oplus S(x \oplus \alpha) = \beta\} \leq \delta \ \forall \alpha, \beta \neq 0$$

δ-uniformidad

Una permutación $S : \mathbb{Z}_2^n \mapsto \mathbb{Z}_2^n$ se dice δ-uniforme si:

$$\#\{x \in \mathbb{Z}_2^n : S(x) \oplus S(x \oplus \alpha) = \beta\} \leq \delta \; \forall \alpha, \beta \neq 0$$

- Un ataque DC busca la entrada no trivial con mayor valor, para tener la probabilidad más favorable y desde el punto de vista del defensor, se quiere una δ-uniformidad con el δ mas chico posible.

δ-uniformidad

Una permutación $S : \mathbb{Z}_2^n \mapsto \mathbb{Z}_2^n$ se dice δ-uniforme si:

$$\#\{x \in \mathbb{Z}_2^n : S(x) \oplus S(x \oplus \alpha) = \beta\} \leq \delta \; \forall \alpha, \beta \neq 0$$

- Un ataque DC busca la entrada no trivial con mayor valor, para tener la probabilidad más favorable y desde el punto de vista del defensor, se quiere una δ-uniformidad con el δ mas chico posible.
- En el caso del xor:
  - x solución de $S(x \oplus \alpha) \oplus S(x) = \beta$

δ-uniformidad

Una permutación $S : \mathbb{Z}_2^n \mapsto \mathbb{Z}_2^n$ se dice δ-uniforme si:

$$\#\{x \in \mathbb{Z}_2^n : S(x) \oplus S(x \oplus \alpha) = \beta\} \leq \delta \ \forall \alpha, \beta \neq 0$$

- Un ataque DC busca la entrada no trivial con mayor valor, para tener la probabilidad más favorable y desde el punto de vista del defensor, se quiere una δ-uniformidad con el δ mas chico posible.
- En el caso del xor:
  - x solución de $S(x \oplus \alpha) \oplus S(x) = \beta \ \Rightarrow x \oplus \alpha$ también es solución

δ-uniformidad

Una permutación $S : \mathbb{Z}_2^n \mapsto \mathbb{Z}_2^n$ se dice δ-uniforme si:

$$\#\{x \in \mathbb{Z}_2^n : S(x) \oplus S(x \oplus \alpha) = \beta\} \leq \delta \ \forall \alpha, \beta \neq 0$$

- Un ataque DC busca la entrada no trivial con mayor valor, para tener la probabilidad más favorable y desde el punto de vista del defensor, se quiere una δ-uniformidad con el δ mas chico posible.
- En el caso del xor:
  - x solución de $S(x \oplus \alpha) \oplus S(x) = \beta \ \Rightarrow x \oplus \alpha$ también es solución pues $S((x \oplus \alpha) \oplus \alpha) \oplus S(x \oplus \alpha)$

δ-uniformidad

Una permutación $S : \mathbb{Z}_2^n \mapsto \mathbb{Z}_2^n$ se dice δ-uniforme si:

$$\#\{x \in \mathbb{Z}_2^n : S(x) \oplus S(x \oplus \alpha) = \beta\} \leq \delta \ \forall \alpha, \beta \neq 0$$

- Un ataque DC busca la entrada no trivial con mayor valor, para tener la probabilidad más favorable y desde el punto de vista del defensor, se quiere una δ-uniformidad con el δ mas chico posible.
- En el caso del xor:
  - x solución de $S(x \oplus \alpha) \oplus S(x) = \beta \ \Rightarrow x \oplus \alpha$ también es solución pues $S((x \oplus \alpha) \oplus \alpha) \oplus S(x \oplus \alpha) = S(x) \oplus S(x \oplus \alpha) = \beta$.

δ-uniformidad

Una permutación $S : \mathbb{Z}_2^n \mapsto \mathbb{Z}_2^n$ se dice δ-uniforme si:

$$\#\{x \in \mathbb{Z}_2^n : S(x) \oplus S(x \oplus \alpha) = \beta\} \leq \delta \; \forall \alpha, \beta \neq 0$$

- Un ataque DC busca la entrada no trivial con mayor valor, para tener la probabilidad más favorable y desde el punto de vista del defensor, se quiere una δ-uniformidad con el δ mas chico posible.
- En el caso del xor:
  - x solución de $S(x \oplus \alpha) \oplus S(x) = \beta \;\Rightarrow x \oplus \alpha$ también es solución pues $S((x \oplus \alpha) \oplus \alpha) \oplus S(x \oplus \alpha) = S(x) \oplus S(x \oplus \alpha) = \beta$.
  - Cualquier entrada en la tabla de diferencias debe ser PAR.

δ-uniformidad

Una permutación $S : \mathbb{Z}_2^n \mapsto \mathbb{Z}_2^n$ se dice δ-uniforme si:

$$\#\{x \in \mathbb{Z}_2^n : S(x) \oplus S(x \oplus \alpha) = \beta\} \leq \delta \; \forall \alpha, \beta \neq 0$$

- Un ataque DC busca la entrada no trivial con mayor valor, para tener la probabilidad más favorable y desde el punto de vista del defensor, se quiere una δ-uniformidad con el δ mas chico posible.
- En el caso del xor:
  - x solución de $S(x \oplus \alpha) \oplus S(x) = \beta \Rightarrow x \oplus \alpha$ también es solución pues $S((x \oplus \alpha) \oplus \alpha) \oplus S(x \oplus \alpha) = S(x) \oplus S(x \oplus \alpha) = \beta$.
  - Cualquier entrada en la tabla de diferencias debe ser PAR.
  - Lo mejor que podemos esperar es 2-uniformidad, y si no se puede, lo siguiente mejor seria 4-uniformidad.

Sboxes activos

Definition

Un Sbox *activo* es un Sbox con diferencia de entradas distinta de 0.

Sboxes activos

Definition

Un Sbox *activo* es un Sbox con diferencia de entradas distinta de 0.

- Cada Sbox activo contribuirá con una probabilidad casi siempre menor a 1 a la probabilidad total,

Sboxes activos

Definition

Un Sbox *activo* es un Sbox con diferencia de entradas distinta de 0.

- Cada Sbox activo contribuirá con una probabilidad casi siempre menor a 1 a la probabilidad total,
- Atacante quiere la menor cantidad de Sboxes activos

Sboxes activos

Definition

Un Sbox *activo* es un Sbox con diferencia de entradas distinta de 0.

- Cada Sbox activo contribuirá con una probabilidad casi siempre menor a 1 a la probabilidad total,
- Atacante quiere la menor cantidad de Sboxes activos
- Defensor quiere crear una estructura que obligue a cualquier ataque a multiplicar el número de Sboxes activos.

Sboxes activos

Definition

Un Sbox *activo* es un Sbox con diferencia de entradas distinta de 0.

- Cada Sbox activo contribuirá con una probabilidad casi siempre menor a 1 a la probabilidad total,
- Atacante quiere la menor cantidad de Sboxes activos
- Defensor quiere crear una estructura que obligue a cualquier ataque a multiplicar el número de Sboxes activos.
- Probar que un diseño logra esto requiere extensivos tests bajo todas las variaciones para mostrar que hay una cierta cantidad mínima de Sboxes activos en una cierta cantidad de rondas.

Sboxes activos

Definition

Un Sbox *activo* es un Sbox con diferencia de entradas distinta de 0.

- Cada Sbox activo contribuirá con una probabilidad casi siempre menor a 1 a la probabilidad total,
- Atacante quiere la menor cantidad de Sboxes activos
- Defensor quiere crear una estructura que obligue a cualquier ataque a multiplicar el número de Sboxes activos.
- Probar que un diseño logra esto requiere extensivos tests bajo todas las variaciones para mostrar que hay una cierta cantidad mínima de Sboxes activos en una cierta cantidad de rondas.
- Por ejemplo, eso es lo que se hace en el cifrador Serpent (que salió segundo en la competencia AES)

La matriz de Rijndael

- Pero Rijmen y Daemen eligieron un diseño que permite dar una demostración matemática de la cota de Sboxes activos, usando el hecho que la multiplicación por la matriz es en un cuerpo finito, y eligiendo cuidadosamente la matriz.

La matriz de Rijndael

- Pero Rijmen y Daemen eligieron un diseño que permite dar una demostración matemática de la cota de Sboxes activos, usando el hecho que la multiplicación por la matriz es en un cuerpo finito, y eligiendo cuidadosamente la matriz.
- La matriz M elegida tiene la propiedad de que cualquier submatriz cuadrada es invertible, es lo que se llama una matriz **MDS**.

La matriz de Rijndael

- Pero Rijmen y Daemen eligieron un diseño que permite dar una demostración matemática de la cota de Sboxes activos, usando el hecho que la multiplicación por la matriz es en un cuerpo finito, y eligiendo cuidadosamente la matriz.
- La matriz M elegida tiene la propiedad de que cualquier submatriz cuadrada es invertible, es lo que se llama una matriz **MDS**.
- El nombre viene de “Maximum Distance Separable" (codes) y viene de la teoría de códigos correctores de errores.

Branch Number

- $\forall x \in GF(2^8)^4$, $x \neq 0$, la suma del número de bytes no nulos de x mas los bytes no nulos de Mx es al menos 5.

Branch Number

- $\forall x \in GF(2^8)^4$, $x \neq 0$, la suma del número de bytes no nulos de x mas los bytes no nulos de Mx es al menos 5.
- (M tiene “branch number" igual a 5).

Branch Number

- $\forall x \in GF(2^8)^4$, $x \neq 0$, la suma del número de bytes no nulos de x mas los bytes no nulos de Mx es al menos 5.
- (M tiene “branch number" igual a 5).
- Es decir:

Branch Number

- $\forall x \in GF(2^8)^4$, $x \neq 0$, la suma del número de bytes no nulos de x mas los bytes no nulos de Mx es al menos 5.
- (M tiene “branch number" igual a 5).
- Es decir:
  - cualquier vector con sólo un byte no nulo producirá un vector con los 4 bytes no nulos,

Branch Number

- $\forall x \in GF(2^8)^4$, $x \neq 0$, la suma del número de bytes no nulos de x mas los bytes no nulos de Mx es al menos 5.
- (M tiene “branch number" igual a 5).
- Es decir:
  - cualquier vector con sólo un byte no nulo producirá un vector con los 4 bytes no nulos,
  - cualquier vector con exactamente dos bytes no nulos producirá un vector con al menos 3 bytes no nulos,

Branch Number

- $\forall x \in GF(2^8)^4$, $x \neq 0$, la suma del número de bytes no nulos de x mas los bytes no nulos de Mx es al menos 5.
- (M tiene “branch number" igual a 5).
- Es decir:
  - cualquier vector con sólo un byte no nulo producirá un vector con los 4 bytes no nulos,
  - cualquier vector con exactamente dos bytes no nulos producirá un vector con al menos 3 bytes no nulos,
  - etc

Branch Number

- $\forall x \in GF(2^8)^4$, $x \neq 0$, la suma del número de bytes no nulos de x mas los bytes no nulos de Mx es al menos 5.
- (M tiene “branch number" igual a 5).
- Es decir:
  - cualquier vector con sólo un byte no nulo producirá un vector con los 4 bytes no nulos,
  - cualquier vector con exactamente dos bytes no nulos producirá un vector con al menos 3 bytes no nulos,
  - etc
- Branch number igual a 5 es lo mejor que se puede esperar de una matriz 4×4

El Lema de Rijmen y Daemen

- Usando esta propiedad de la matriz, mas una propiedad de la permutación de bytes incorporada a AES, Rijmen y Daemen probaron el siguiente:

El Lema de Rijmen y Daemen

- Usando esta propiedad de la matriz, mas una propiedad de la permutación de bytes incorporada a AES, Rijmen y Daemen probaron el siguiente:

Lema

En cualquier ataque diferencial, en cuatro rondas consecutivas de Rijndael hay al menos 25 S-boxes activos.

El Lema de Rijmen y Daemen

- Usando esta propiedad de la matriz, mas una propiedad de la permutación de bytes incorporada a AES, Rijmen y Daemen probaron el siguiente:

Lema

En cualquier ataque diferencial, en cuatro rondas consecutivas de Rijndael hay al menos 25 S-boxes activos.

No probaremos esto pues nos llevaria bastante tiempo. Pero esto es sólo una de las patas de la resistencia de AES. Ademas, necesitamos que el Sbox sea resistente.

Como hallar Sboxes “buenos"

- Para n par, sólo se conoce un Sbox 2-uniforme, para el caso $n = 6$, pero en general es conveniente usar n's que sean potencia de 2. (ademas que ese de $n = 6$ es de la NSA)

Como hallar Sboxes “buenos"

- Para n par, sólo se conoce un Sbox 2-uniforme, para el caso $n = 6$, pero en general es conveniente usar n's que sean potencia de 2. (ademas que ese de $n = 6$ es de la NSA)
- Para $n = 4$ es fácil encontrar Sboxes 4-uniformes buscando al azar.

Como hallar Sboxes “buenos"

- Para n par, sólo se conoce un Sbox 2-uniforme, para el caso $n = 6$, pero en general es conveniente usar n's que sean potencia de 2. (ademas que ese de $n = 6$ es de la NSA)
- Para $n = 4$ es fácil encontrar Sboxes 4-uniformes buscando al azar.
- Para $n = 8$ esto no parece ser posible. (hasta ahora, buscando al azar por largo tiempo, no se han encontrado).

Como hallar Sboxes “buenos"

- Para n par, sólo se conoce un Sbox 2-uniforme, para el caso $n = 6$, pero en general es conveniente usar n's que sean potencia de 2. (ademas que ese de $n = 6$ es de la NSA)
- Para $n = 4$ es fácil encontrar Sboxes 4-uniformes buscando al azar.
- Para $n = 8$ esto no parece ser posible. (hasta ahora, buscando al azar por largo tiempo, no se han encontrado).
- Pero se pueden construir matemáticamente, usando cuerpos finitos.

Teorema de Nyberg

Teorema de Nyberg

Teorema de Nyberg

Teorema de Nyberg

Sea S el S-box dado por $S(x) = x^{-1}$ si $x \neq 0$ y $S(0) = 0$, donde la inversión se hace en el cuerpo finito $GF(2^n)$.

Teorema de Nyberg

Teorema de Nyberg

Sea S el S-box dado por $S(x) = x^{-1}$ si $x \neq 0$ y $S(0) = 0$, donde la inversión se hace en el cuerpo finito $GF(2^n)$.
Las mayores probabilidades diferenciales no triviales son menores o iguales a 2^{-n+2}.

Teorema de Nyberg

Teorema de Nyberg

Sea S el S-box dado por $S(x) = x^{-1}$ si $x \neq 0$ y $S(0) = 0$, donde la inversión se hace en el cuerpo finito $GF(2^n)$.
Las mayores probabilidades diferenciales no triviales son menores o iguales a 2^{-n+2}.
Ademas, en el caso impar la mayor probabilidad diferencial es menor o igual a 2^{-n+1}.

Teorema de Nyberg

Teorema de Nyberg

Sea S el S-box dado por $S(x) = x^{-1}$ si $x \neq 0$ y $S(0) = 0$, donde la inversión se hace en el cuerpo finito $GF(2^n)$.
Las mayores probabilidades diferenciales no triviales son menores o iguales a 2^{-n+2}.
Ademas, en el caso impar la mayor probabilidad diferencial es menor o igual a 2^{-n+1}.
Es decir, S es 2-uniforme si n es impar y 4-uniforme (pero no 2 uniforme) si n es par.

Teorema de Nyberg

Prueba:

Teorema de Nyberg

Prueba:

- Dados $\alpha, \beta \neq 0$, queremos contar el número de soluciones de la ecuación $S(x) \oplus S(x \oplus \alpha) = \beta$.

Teorema de Nyberg

Prueba:

- Dados $\alpha, \beta \neq 0$, queremos contar el número de soluciones de la ecuación $S(x) \oplus S(x \oplus \alpha) = \beta$.
- si $\beta = \alpha^{-1}$, tenemos las dos soluciones $x = 0, \alpha$, pues $S(0) \oplus S(\alpha) = 0 \oplus \alpha^{-1} = \beta$.

Teorema de Nyberg

Prueba:

- Dados $\alpha, \beta \neq 0$, queremos contar el número de soluciones de la ecuación $S(x) \oplus S(x \oplus \alpha) = \beta$.
- si $\beta = \alpha^{-1}$, tenemos las dos soluciones $x = 0, \alpha$, pues $S(0) \oplus S(\alpha) = 0 \oplus \alpha^{-1} = \beta$.
- Si $\beta \neq \alpha^{-1}$ entonces 0 y α no son soluciones.

Teorema de Nyberg

Prueba:

- Dados $\alpha, \beta \neq 0$, queremos contar el número de soluciones de la ecuación $S(x) \oplus S(x \oplus \alpha) = \beta$.
- si $\beta = \alpha^{-1}$, tenemos las dos soluciones $x = 0, \alpha$, pues $S(0) \oplus S(\alpha) = 0 \oplus \alpha^{-1} = \beta$.
- Si $\beta \neq \alpha^{-1}$ entonces 0 y α no son soluciones.
- Independientemente que lo sean o no, queremos contar cuantas otras soluciones hay.

Nyberg cont.

Sea $x \neq 0, \alpha$.

Nyberg cont.

Sea $x \neq 0, \alpha$.

$$S(x) \oplus S(x \oplus \alpha) \quad = \quad x^{-1} \oplus (x \oplus \alpha)^{-1}$$

Nyberg cont.

Sea $x \neq 0, \alpha$.

$$\begin{aligned} S(x) \oplus S(x \oplus \alpha) &= x^{-1} \oplus (x \oplus \alpha)^{-1} \\ &= (x \oplus \alpha)(x \oplus \alpha)^{-1} x^{-1} \oplus x x^{-1} (x \oplus \alpha)^{-1} \end{aligned}$$

Nyberg cont.

Sea $x \neq 0, \alpha$.

$$\begin{aligned} S(x) \oplus S(x \oplus \alpha) &= x^{-1} \oplus (x \oplus \alpha)^{-1} \\ &= (x \oplus \alpha)(x \oplus \alpha)^{-1} x^{-1} \oplus x x^{-1} (x \oplus \alpha)^{-1} \\ &= (x \oplus \alpha)^{-1} x^{-1} ((x \oplus \alpha) \oplus x) \end{aligned}$$

Nyberg cont.

Sea $x \neq 0, \alpha$.

$$\begin{aligned} S(x) \oplus S(x \oplus \alpha) &= x^{-1} \oplus (x \oplus \alpha)^{-1} \\ &= (x \oplus \alpha)(x \oplus \alpha)^{-1} x^{-1} \oplus x x^{-1} (x \oplus \alpha)^{-1} \\ &= (x \oplus \alpha)^{-1} x^{-1} ((x \oplus \alpha) \oplus x) \\ &= (x(x \oplus \alpha))^{-1} \alpha \end{aligned}$$

Nyberg cont.

Sea $x \neq 0, \alpha$.

$$\begin{aligned} S(x) \oplus S(x \oplus \alpha) &= x^{-1} \oplus (x \oplus \alpha)^{-1} \\ &= (x \oplus \alpha)(x \oplus \alpha)^{-1} x^{-1} \oplus x x^{-1} (x \oplus \alpha)^{-1} \\ &= (x \oplus \alpha)^{-1} x^{-1} ((x \oplus \alpha) \oplus x) \\ &= (x(x \oplus \alpha))^{-1} \alpha \end{aligned}$$

Por lo tanto $S(x) \oplus S(x \oplus \alpha) = \beta$ si y solo si $(x(x \oplus \alpha))^{-1} \alpha = \beta$

Nyberg cont.

Sea $x \neq 0, \alpha$.

$$\begin{aligned} S(x) \oplus S(x \oplus \alpha) &= x^{-1} \oplus (x \oplus \alpha)^{-1} \\ &= (x \oplus \alpha)(x \oplus \alpha)^{-1} x^{-1} \oplus x x^{-1} (x \oplus \alpha)^{-1} \\ &= (x \oplus \alpha)^{-1} x^{-1} ((x \oplus \alpha) \oplus x) \\ &= (x(x \oplus \alpha))^{-1} \alpha \end{aligned}$$

Por lo tanto $S(x) \oplus S(x \oplus \alpha) = \beta$ si y solo si $(x(x \oplus \alpha))^{-1} \alpha = \beta$ si y solo si $\alpha = x(x \oplus \alpha)\beta$

- El número de x's que satisface la ecuación $\alpha = x(x \oplus \alpha)\beta$ es a lo sumo 2, pues es un polinomio de segundo grado y estamos en un cuerpo.

- El número de x's que satisface la ecuación $\alpha = x(x \oplus \alpha)\beta$ es a lo sumo 2, pues es un polinomio de segundo grado y estamos en un cuerpo.
- A estas dos posibles soluciones hay que sumarles dos mas si $\alpha\beta = 1$.

- El número de x's que satisface la ecuación $\alpha = x(x \oplus \alpha)\beta$ es a lo sumo 2, pues es un polinomio de segundo grado y estamos en un cuerpo.
- A estas dos posibles soluciones hay que sumarles dos mas si $\alpha\beta = 1$.
- En resumen, el número total de soluciones es:

- El número de x's que satisface la ecuación $\alpha = x(x \oplus \alpha)\beta$ es a lo sumo 2, pues es un polinomio de segundo grado y estamos en un cuerpo.
- A estas dos posibles soluciones hay que sumarles dos mas si $\alpha\beta = 1$.
- En resumen, el número total de soluciones es:
  - 0 o 2 si $\beta \neq \alpha^{-1}$

- El número de x's que satisface la ecuación $\alpha = x(x \oplus \alpha)\beta$ es a lo sumo 2, pues es un polinomio de segundo grado y estamos en un cuerpo.
- A estas dos posibles soluciones hay que sumarles dos mas si $\alpha\beta = 1$.
- En resumen, el número total de soluciones es:
  - 0 o 2 si $\beta \neq \alpha^{-1}$
  - 2 o 4 si $\beta = \alpha^{-1}$

- El número de x's que satisface la ecuación $\alpha = x(x \oplus \alpha)\beta$ es a lo sumo 2, pues es un polinomio de segundo grado y estamos en un cuerpo.
- A estas dos posibles soluciones hay que sumarles dos mas si $\alpha\beta = 1$.
- En resumen, el número total de soluciones es:
  - 0 o 2 si $\beta \neq \alpha^{-1}$
  - 2 o 4 si $\beta = \alpha^{-1}$
- ¿Cuando se da que hay 4 soluciones?

Condicion para que existan 4 soluciones

Propiedad

El Sbox de Nyberg es 2-uniforme si y solo si no existe z con $z^2 \oplus z = 1$

- Como acabamos de ver la única posibilidad de que el Sbox de Nyberg no sea 2-uniforme es que exista alguna solución $x \neq 0, \alpha$ de la ecuación $S(x) \oplus S(x \oplus \alpha) = \beta$ cuando $\beta = \alpha^{-1}$

Condicion para que existan 4 soluciones

Propiedad

El Sbox de Nyberg es 2-uniforme si y solo si no existe z con $z^2 \oplus z = 1$

- Como acabamos de ver la única posibilidad de que el Sbox de Nyberg no sea 2-uniforme es que exista alguna solución $x \neq 0, \alpha$ de la ecuación $S(x) \oplus S(x \oplus \alpha) = \beta$ cuando $\beta = \alpha^{-1}$
- Por la cuenta anterior, tal x debe satisfacer $\alpha = x(x \oplus \alpha)\beta$

Condicion para que existan 4 soluciones

Propiedad

El Sbox de Nyberg es 2-uniforme si y solo si no existe z con $z^2 \oplus z = 1$

- Como acabamos de ver la única posibilidad de que el Sbox de Nyberg no sea 2-uniforme es que exista alguna solución $x \neq 0, \alpha$ de la ecuación $S(x) \oplus S(x \oplus \alpha) = \beta$ cuando $\beta = \alpha^{-1}$
- Por la cuenta anterior, tal x debe satisfacer $\alpha = x(x \oplus \alpha)\beta$
- Como $\beta = \alpha^{-1}$ esto ocurre si y solo si $\alpha = x(x \oplus \alpha)\alpha^{-1}$

Condicion para que existan 4 soluciones

Propiedad

El Sbox de Nyberg es 2-uniforme si y solo si no existe z con $z^2 \oplus z = 1$

- Como acabamos de ver la única posibilidad de que el Sbox de Nyberg no sea 2-uniforme es que exista alguna solución $x \neq 0, \alpha$ de la ecuación $S(x) \oplus S(x \oplus \alpha) = \beta$ cuando $\beta = \alpha^{-1}$
- Por la cuenta anterior, tal x debe satisfacer $\alpha = x(x \oplus \alpha)\beta$
- Como $\beta = \alpha^{-1}$ esto ocurre si y solo si $\alpha = x(x \oplus \alpha)\alpha^{-1}$
- Si y solo si $1 = (x\alpha^{-1})(x\alpha^{-1} \oplus 1)$.

Condicion para que existan 4 soluciones

Propiedad

El Sbox de Nyberg es 2-uniforme si y solo si no existe z con $z^2 \oplus z = 1$

- Como acabamos de ver la única posibilidad de que el Sbox de Nyberg no sea 2-uniforme es que exista alguna solución $x \neq 0, \alpha$ de la ecuación $S(x) \oplus S(x \oplus \alpha) = \beta$ cuando $\beta = \alpha^{-1}$
- Por la cuenta anterior, tal x debe satisfacer $\alpha = x(x \oplus \alpha)\beta$
- Como $\beta = \alpha^{-1}$ esto ocurre si y solo si $\alpha = x(x \oplus \alpha)\alpha^{-1}$
- Si y solo si $1 = (x\alpha^{-1})(x\alpha^{-1} \oplus 1)$.
- Sea $z = x\alpha^{-1}$. Por lo anterior $1 = z(z \oplus 1) = z^2 \oplus z$.

Condicion para que existan 4 soluciones

Propiedad

El Sbox de Nyberg es 2-uniforme si y solo si no existe z con $z^2 \oplus z = 1$

- Como acabamos de ver la única posibilidad de que el Sbox de Nyberg no sea 2-uniforme es que exista alguna solución $x \neq 0, \alpha$ de la ecuación $S(x) \oplus S(x \oplus \alpha) = \beta$ cuando $\beta = \alpha^{-1}$
- Por la cuenta anterior, tal x debe satisfacer $\alpha = x(x \oplus \alpha)\beta$
- Como $\beta = \alpha^{-1}$ esto ocurre si y solo si $\alpha = x(x \oplus \alpha)\alpha^{-1}$
- Si y solo si $1 = (x\alpha^{-1})(x\alpha^{-1} \oplus 1)$.
- Sea $z = x\alpha^{-1}$. Por lo anterior $1 = z(z \oplus 1) = z^2 \oplus z$.
- Viceversa, si z es tal que $z^2 \oplus z = 1$, definimos $x = \alpha z$ y entonces $1 = (x\alpha^{-1})(x\alpha^{-1} \oplus 1)$

2-uniformidad en el caso impar.

- Veamos que en el caso n impar, no existen 4 soluciones, i.e., el Sbox es 2-uniforme.

2-uniformidad en el caso impar.

- Veamos que en el caso n impar, no existen 4 soluciones, i.e., el Sbox es 2-uniforme.
- Si existieran 4 soluciones, por lo anterior existe z con $z^2 \oplus z = 1$.

2-uniformidad en el caso impar.

- Veamos que en el caso n impar, no existen 4 soluciones, i.e., el Sbox es 2-uniforme.
- Si existieran 4 soluciones, por lo anterior existe z con $z^2 \oplus z = 1$.
- Como $(GF(2^n) - \{0\}, .)$ es un grupo con $2^n - 1$ elementos tendremos que $z^{2^n-1} = 1$ (teorema de Lagrange)

2-uniformidad en el caso impar.

- Veamos que en el caso n impar, no existen 4 soluciones, i.e., el Sbox es 2-uniforme.
- Si existieran 4 soluciones, por lo anterior existe z con $z^2 \oplus z = 1$.
- Como $(GF(2^n) - \{0\}, .)$ es un grupo con $2^n - 1$ elementos tendremos que $z^{2^n-1} = 1$ (teorema de Lagrange)
- Es decir, $z^{2^n} = z$ y $z^{2^n} \oplus z = 0$.

2-uniformidad en el caso impar.

- Veamos que en el caso n impar, no existen 4 soluciones, i.e., el Sbox es 2-uniforme.
- Si existieran 4 soluciones, por lo anterior existe z con $z^2 \oplus z = 1$.
- Como $(GF(2^n) - \{0\}, .)$ es un grupo con $2^n - 1$ elementos tendremos que $z^{2^n-1} = 1$ (teorema de Lagrange)
- Es decir, $z^{2^n} = z$ y $z^{2^n} \oplus z = 0$.
- Por otro lado, recordemos que $(a \oplus b)^2 = a^2 \oplus b^2$ en $GF(2^n)$.

2-uniformidad en el caso impar.

- Veamos que en el caso n impar, no existen 4 soluciones, i.e., el Sbox es 2-uniforme.
- Si existieran 4 soluciones, por lo anterior existe z con $z^2 \oplus z = 1$.
- Como $(GF(2^n) - \{0\}, .)$ es un grupo con $2^n - 1$ elementos tendremos que $z^{2^n-1} = 1$ (teorema de Lagrange)
- Es decir, $z^{2^n} = z$ y $z^{2^n} \oplus z = 0$.
- Por otro lado, recordemos que $(a \oplus b)^2 = a^2 \oplus b^2$ en $GF(2^n)$.
- Por lo tanto, elevando al cuadrado la ecuación $1 = z^2 \oplus z$ obtenemos $1 = z^4 \oplus z^2$

2-uniformidad en el caso impar.

- Veamos que en el caso n impar, no existen 4 soluciones, i.e., el Sbox es 2-uniforme.
- Si existieran 4 soluciones, por lo anterior existe z con $z^2 \oplus z = 1$.
- Como $(GF(2^n) - \{0\}, .)$ es un grupo con $2^n - 1$ elementos tendremos que $z^{2^n-1} = 1$ (teorema de Lagrange)
- Es decir, $z^{2^n} = z$ y $z^{2^n} \oplus z = 0$.
- Por otro lado, recordemos que $(a \oplus b)^2 = a^2 \oplus b^2$ en $GF(2^n)$.
- Por lo tanto, elevando al cuadrado la ecuación $1 = z^2 \oplus z$ obtenemos $1 = z^4 \oplus z^2$
- continuemos elevando al cuadrado repetidamente

2-uniformidad en el caso impar (cont).

$$z^2 \oplus z = \qquad\qquad 1$$

2-uniformidad en el caso impar (cont).

$$z^2 \oplus z = 1$$
$$z^4 \oplus z^2 = 1$$

2-uniformidad en el caso impar (cont).

$$
\begin{aligned}
z^2 \oplus z &= 1 \\
z^4 \oplus z^2 &= 1 \\
z^8 \oplus z^4 &= 1
\end{aligned}
$$

2-uniformidad en el caso impar (cont).

$$
\begin{aligned}
z^2 \oplus z &= 1 \\
z^4 \oplus z^2 &= 1 \\
z^8 \oplus z^4 &= 1 \\
&\vdots \quad\quad \vdots \\
z^{2^{n-1}} \oplus z^{2^{n-2}} &= 1
\end{aligned}
$$

2-uniformidad en el caso impar (cont).

$$
\begin{aligned}
z^2 \oplus z &= 1 \\
z^4 \oplus z^2 &= 1 \\
z^8 \oplus z^4 &= 1 \\
&\vdots \qquad\quad \vdots \\
z^{2^{n-1}} \oplus z^{2^{n-2}} &= 1 \\
z^{2^n} \oplus z^{2^{n-1}} &= 1
\end{aligned}
$$

2-uniformidad en el caso impar (cont).

$$
\begin{aligned}
z^2 \oplus z &= 1 \\
z^4 \oplus z^2 &= 1 \\
z^8 \oplus z^4 &= 1 \\
&\vdots \quad \vdots \\
z^{2^{n-1}} \oplus z^{2^{n-2}} &= 1 \\
z^{2^n} \oplus z^{2^{n-1}} &= 1 \\
- - - - - - - - - &= - -
\end{aligned}
$$

$$
=
$$

2-uniformidad en el caso impar (cont).

$$
\begin{aligned}
\not{z}^2 \oplus z &= & 1 \\
z^4 \oplus \ \not{z}^2 &= & 1 \\
z^8 \oplus z^4 &= & 1 \\
&\vdots & \vdots \\
z^{2^{n-1}} \oplus z^{2^{n-2}} &= & 1 \\
z^{2^n} \oplus z^{2^{n-1}} &= & 1 \\
------------- &= & -- \\
&= &
\end{aligned}
$$

2-uniformidad en el caso impar (cont).

$$
\begin{array}{rcc}
\not{z}^2 \oplus z & = & 1 \\
\not{z}^4 \oplus \not{z}^2 & = & 1 \\
z^8 \oplus \not{z}^4 & = & 1 \\
\vdots & & \vdots \\
z^{2^{n-1}} \oplus z^{2^{n-2}} & = & 1 \\
z^{2^n} \oplus z^{2^{n-1}} & = & 1 \\
- - - - - - - - - & = & - - \\
 & = &
\end{array}
$$

2-uniformidad en el caso impar (cont).

$$
\begin{aligned}
\not{z}^2 \oplus z &= 1 \\
\not{z}^4 \oplus \not{z}^2 &= 1 \\
\not{z}^8 \oplus \not{z}^4 &= 1 \\
&\vdots \quad\quad \vdots \\
z^{2^{n-1}} \oplus z^{2^{n-2}} &= 1 \\
z^{2^n} \oplus z^{2^{n-1}} &= 1 \\
- - - - - - - - - &= - -
\end{aligned}
$$

$$
=
$$

2-uniformidad en el caso impar (cont).

$$
\begin{aligned}
\not{z}^2 \oplus z &= 1 \\
\not{z}^4 \oplus \not{z}^2 &= 1 \\
\not{z}^8 \oplus \not{z}^4 &= 1 \\
&\vdots \quad\quad \vdots \\
z^{2^{n-1}} \oplus \not{z}^{2^{n-2}} &= 1 \\
z^{2^n} \oplus z^{2^{n-1}} &= 1 \\
- - - - - - - - - &= - -
\end{aligned}
$$

$$
=
$$

2-uniformidad en el caso impar (cont).

$$
\begin{array}{rcl}
\not{z}^2 \oplus z = & & 1 \\
\not{z}^4 \oplus \not{z}^2 = & & 1 \\
\not{z}^8 \oplus \not{z}^4 = & & 1 \\
\vdots & & \vdots \\
\not{z}^{2^{n-1}} \oplus \not{z}^{2^{n-2}} = & & 1 \\
z^{2^n} \oplus \not{z}^{2^{n-1}} = & & 1 \\
- - - - - - - - - = & & - - \\
 & = & \\
 & = &
\end{array}
$$

2-uniformidad en el caso impar (cont).

$$
\begin{array}{rcl}
\not{z}^2 \oplus z & = & 1 \\
\not{z}^4 \oplus \not{z}^2 & = & 1 \\
\not{z}^8 \oplus \not{z}^4 & = & 1 \\
\vdots & & \vdots \\
\not{z}^{2^{n-1}} \oplus \not{z}^{2^{n-2}} & = & 1 \\
z^{2^n} \oplus \not{z}^{2^{n-1}} & = & 1 \\
- - - - - - - - - & = & - - \\
 & = &
\end{array}
$$

2-uniformidad en el caso impar (cont).

$$
\begin{array}{rcl}
\not{z}^2 \oplus z = & & 1 \\
\not{z}^4 \oplus \not{z}^2 = & & 1 \\
\not{z}^8 \oplus \not{z}^4 = & & 1 \\
\vdots & & \vdots \\
\not{z}^{2^{n-1}} \oplus \not{z}^{2^{n-2}} = & & 1 \\
z^{2^n} \oplus \not{z}^{2^{n-1}} = & & 1 \\
- - - - - - - - - = & & - -
\end{array}
$$

$$
z^{2^n} \oplus z =
$$

2-uniformidad en el caso impar (cont).

$$
\begin{aligned}
\not{z}^2 \oplus z &= 1 \\
\not{z}^4 \oplus \not{z}^2 &= 1 \\
\not{z}^8 \oplus \not{z}^4 &= 1 \\
&\vdots \quad \vdots \\
\not{z}^{2^{n-1}} \oplus \not{z}^{2^{n-2}} &= 1 \\
z^{2^n} \oplus \not{z}^{2^{n-1}} &= 1 \\
- - - - - - - - - - &= - -
\end{aligned}
$$

$$z^{2^n} \oplus z = 0 =$$

2-uniformidad en el caso impar (cont).

$$
\begin{aligned}
\not{z}^2 \oplus z &= 1 \\
\not{z}^4 \oplus \not{z}^2 &= 1 \\
\not{z}^8 \oplus \not{z}^4 &= 1 \\
&\vdots \quad\quad \vdots \\
\not{z}^{2^{n-1}} \oplus \not{z}^{2^{n-2}} &= 1 \\
z^{2^n} \oplus \not{z}^{2^{n-1}} &= 1 \\
- - - - - - - - - - &= - - \\
z^{2^n} \oplus z = 0 &= \overbrace{1 \oplus \ldots \oplus 1}^{n}
\end{aligned}
$$

2-uniformidad en el caso impar (cont).

$$
\begin{aligned}
\not{z}^2 \oplus z &= 1 \\
\not{z}^4 \oplus \not{z}^2 &= 1 \\
\not{z}^8 \oplus \not{z}^4 &= 1 \\
&\vdots \quad\quad \vdots \\
\not{z}^{2^{n-1}} \oplus \not{z}^{2^{n-2}} &= 1 \\
z^{2^n} \oplus \not{z}^{2^{n-1}} &= 1 \\
- - - - - - - - - &= - - \\
z^{2^n} \oplus z = 0 &= \overbrace{1 \oplus \ldots \oplus 1}^{n}
\end{aligned}
$$

Como n es impar hay una cantidad impar de terminos en ese xor

2-uniformidad en el caso impar (cont).

$$
\begin{aligned}
\not{z}^2 \oplus z &= 1 \\
\not{z}^4 \oplus \not{z}^2 &= 1 \\
\not{z}^8 \oplus \not{z}^4 &= 1 \\
&\vdots \quad\quad \vdots \\
\not{z}^{2^{n-1}} \oplus \not{z}^{2^{n-2}} &= 1 \\
z^{2^n} \oplus \not{z}^{2^{n-1}} &= 1 \\
- - - - - - - - - &= - -
\end{aligned}
$$

$$
z^{2^n} \oplus z = 0 = 1 = \overbrace{1 \oplus \ldots \oplus 1}^{n}
$$

Como n es impar hay una cantidad impar de terminos en ese xor

2-uniformidad en el caso impar (cont).

$$
\begin{aligned}
\not{z}^2 \oplus z &= 1 \\
\not{z}^4 \oplus \not{z}^2 &= 1 \\
\not{z}^8 \oplus \not{z}^4 &= 1 \\
&\vdots \quad\quad \vdots \\
\not{z}^{2^{n-1}} \oplus \not{z}^{2^{n-2}} &= 1 \\
z^{2^n} \oplus \not{z}^{2^{n-1}} &= 1 \\
- - - - - - - - - &= - -
\end{aligned}
$$

$$
z^{2^n} \oplus z = 0 = 1 = \overbrace{1 \oplus \ldots \oplus 1}^{n}
$$

$0 = 1$, absurdo

No hay 2-uniformidad en el caso par

- El teorema del elemento primitivo dice que en cualquier cuerpo finito existe un elemento primitivo, es decir, un elemento tal que sus potencias generan todos los elementos no nulos del cuerpo.

No hay 2-uniformidad en el caso par

- El teorema del elemento primitivo dice que en cualquier cuerpo finito existe un elemento primitivo, es decir, un elemento tal que sus potencias generan todos los elementos no nulos del cuerpo.
- En el caso de $GF(2^n)$, ρ es un elemento primitivo si y solo si $\rho^t = 1 \Rightarrow (2^n - 1)|t$.

No hay 2-uniformidad en el caso par

- El teorema del elemento primitivo dice que en cualquier cuerpo finito existe un elemento primitivo, es decir, un elemento tal que sus potencias generan todos los elementos no nulos del cuerpo.
- En el caso de $GF(2^n)$, ρ es un elemento primitivo si y solo si $\rho^t = 1 \Rightarrow (2^n - 1)|t$.
- Sea ρ un elemento primitivo de $GF(2^n)$.

No hay 2-uniformidad en el caso par

- El teorema del elemento primitivo dice que en cualquier cuerpo finito existe un elemento primitivo, es decir, un elemento tal que sus potencias generan todos los elementos no nulos del cuerpo.
- En el caso de $GF(2^n)$, ρ es un elemento primitivo si y solo si $\rho^t = 1 \Rightarrow (2^n - 1)|t$.
- Sea ρ un elemento primitivo de $GF(2^n)$.
- Como n es par, es de la forma $n = 2k$. Asi, $2^n - 1 = 4^k - 1$.

No hay 2-uniformidad en el caso par

- El teorema del elemento primitivo dice que en cualquier cuerpo finito existe un elemento primitivo, es decir, un elemento tal que sus potencias generan todos los elementos no nulos del cuerpo.
- En el caso de $GF(2^n)$, ρ es un elemento primitivo si y solo si $\rho^t = 1 \Rightarrow (2^n - 1)|t$.
- Sea ρ un elemento primitivo de $GF(2^n)$.
- Como n es par, es de la forma $n = 2k$. Asi, $2^n - 1 = 4^k - 1$.
- Por lo tanto, $(2^n - 1) \text{mod } 3 = 1^k - 1 = 0$

No hay 2-uniformidad en el caso par

- El teorema del elemento primitivo dice que en cualquier cuerpo finito existe un elemento primitivo, es decir, un elemento tal que sus potencias generan todos los elementos no nulos del cuerpo.
- En el caso de $GF(2^n)$, ρ es un elemento primitivo si y solo si $\rho^t = 1 \Rightarrow (2^n - 1)|t$.
- Sea ρ un elemento primitivo de $GF(2^n)$.
- Como n es par, es de la forma $n = 2k$. Asi, $2^n - 1 = 4^k - 1$.
- Por lo tanto, $(2^n - 1) \text{mod } 3 = 1^k - 1 = 0$
- i.e., 3 divide a $2^n - 1$ ($\Rightarrow \frac{2^n-1}{3}$ es un entero).

No hay 2-uniformidad en el caso par

- El teorema del elemento primitivo dice que en cualquier cuerpo finito existe un elemento primitivo, es decir, un elemento tal que sus potencias generan todos los elementos no nulos del cuerpo.
- En el caso de $GF(2^n)$, ρ es un elemento primitivo si y solo si $\rho^t = 1 \Rightarrow (2^n - 1)|t$.
- Sea ρ un elemento primitivo de $GF(2^n)$.
- Como n es par, es de la forma $n = 2k$. Asi, $2^n - 1 = 4^k - 1$.
- Por lo tanto, $(2^n - 1) \text{mod } 3 = 1^k - 1 = 0$
- i.e., 3 divide a $2^n - 1$ ($\Rightarrow \frac{2^n-1}{3}$ es un entero).
- Tiene sentido entonces tomar el elemento $z = \rho^{\frac{2^n-1}{3}}$

No 2-uniformidad en el caso par (cont)

- $z^3 = (\rho^{\frac{2^n-1}{3}})^3 = \rho^{2^n-1} = 1.$

No 2-uniformidad en el caso par (cont)

- $z^3 = (\rho^{\frac{2^n-1}{3}})^3 = \rho^{2^n-1} = 1.$
- $0 = z^3 \oplus 1 = (z \oplus 1)(z^2 \oplus z \oplus 1)$

No 2-uniformidad en el caso par (cont)

- $z^3 = (\rho^{\frac{2^n-1}{3}})^3 = \rho^{2^n-1} = 1.$
- $0 = z^3 \oplus 1 = (z \oplus 1)(z^2 \oplus z \oplus 1)$
- Como estamos en un cuerpo, un producto de dos factores es 0 si y solo si al menos uno de ellos es cero.

No 2-uniformidad en el caso par (cont)

- $z^3 = (\rho^{\frac{2^n-1}{3}})^3 = \rho^{2^n-1} = 1$.
- $0 = z^3 \oplus 1 = (z \oplus 1)(z^2 \oplus z \oplus 1)$
- Como estamos en un cuerpo, un producto de dos factores es 0 si y solo si al menos uno de ellos es cero.
- Asi que, o bien $z = 1$ o bien $z^2 \oplus z = 1$.

No 2-uniformidad en el caso par (cont)

- $z^3 = (\rho^{\frac{2^n-1}{3}})^3 = \rho^{2^n-1} = 1$.
- $0 = z^3 \oplus 1 = (z \oplus 1)(z^2 \oplus z \oplus 1)$
- Como estamos en un cuerpo, un producto de dos factores es 0 si y solo si al menos uno de ellos es cero.
- Asi que, o bien $z = 1$ o bien $z^2 \oplus z = 1$.
- Como ρ es primitivo $z = \rho^{\frac{2^n-1}{3}}$ no puede ser 1, pues $\frac{2^n-1}{3} < 2^n - 1$.

No 2-uniformidad en el caso par (cont)

- $z^3 = (\rho^{\frac{2^n-1}{3}})^3 = \rho^{2^n-1} = 1$.
- $0 = z^3 \oplus 1 = (z \oplus 1)(z^2 \oplus z \oplus 1)$
- Como estamos en un cuerpo, un producto de dos factores es 0 si y solo si al menos uno de ellos es cero.
- Asi que, o bien $z = 1$ o bien $z^2 \oplus z = 1$.
- Como ρ es primitivo $z = \rho^{\frac{2^n-1}{3}}$ no puede ser 1, pues $\frac{2^n-1}{3} < 2^n - 1$.
- Entonces, debe ser $z^2 \oplus z = 1$ y vimos que esto implica que no puede ser 2-uniforme.

Resistencia de AES al DC

- Rijndael usa un Sbox de Nyberg compuesto con una transformación afín.

Resistencia de AES al DC

- Rijndael usa un Sbox de Nyberg compuesto con una transformación afín.
- Esa composición tiene las mismas propiedades que el Sbox de Nyberg.

Resistencia de AES al DC

- Rijndael usa un Sbox de Nyberg compuesto con una transformación afín.
- Esa composición tiene las mismas propiedades que el Sbox de Nyberg.
- Combinando esto con el Lema de Rijmen y Daemen que vimos antes, se tiene:

Resistencia de AES al DC

- Rijndael usa un Sbox de Nyberg compuesto con una transformación afín.
- Esa composición tiene las mismas propiedades que el Sbox de Nyberg.
- Combinando esto con el Lema de Rijmen y Daemen que vimos antes, se tiene:

Teorema

La probabilidad de cualquier característica diferencial de cuatro rondas en Rijndael es menor o igual a 2^{-150}

Resistencia de AES contra DC

- Prueba del Teorema:

Resistencia de AES contra DC

- Prueba del Teorema:
  - En cualquier ataque diferencial, por el lema de Rijmen y Daemen, debe haber al menos 25 S-boxes con diferencias de entrada no nulas en 4 rondas.

Resistencia de AES contra DC

- Prueba del Teorema:
  - En cualquier ataque diferencial, por el lema de Rijmen y Daemen, debe haber al menos 25 S-boxes con diferencias de entrada no nulas en 4 rondas.
  - Cada uno de esos S-boxes es 4-uniforme, asi que tiene una probabilidad diferencial máxima de $\frac{4}{2^8} = 2^{-6}$

Resistencia de AES contra DC

- Prueba del Teorema:
  - En cualquier ataque diferencial, por el lema de Rijmen y Daemen, debe haber al menos 25 S-boxes con diferencias de entrada no nulas en 4 rondas.
  - Cada uno de esos S-boxes es 4-uniforme, asi que tiene una probabilidad diferencial máxima de $\frac{4}{2^8} = 2^{-6}$
  - Asi, la probabilidad diferencial total es de a lo sumo $(2^{-6})^{25} = 2^{-150}$

Resistencia de AES contra DC

- Prueba del Teorema:
  - En cualquier ataque diferencial, por el lema de Rijmen y Daemen, debe haber al menos 25 S-boxes con diferencias de entrada no nulas en 4 rondas.
  - Cada uno de esos S-boxes es 4-uniforme, asi que tiene una probabilidad diferencial máxima de $\frac{4}{2^8} = 2^{-6}$
  - Asi, la probabilidad diferencial total es de a lo sumo $(2^{-6})^{25} = 2^{-150}$
- Consecuencia del Teorema: Para poder montar un ataque DC con alguna probabilidad de éxito contra 4 rondas de Rijndael, se deben disponer de al menos 2^{150} mensajes de 1 bloque.

Resistencia de AES contra DC

- Prueba del Teorema:
  - En cualquier ataque diferencial, por el lema de Rijmen y Daemen, debe haber al menos 25 S-boxes con diferencias de entrada no nulas en 4 rondas.
  - Cada uno de esos S-boxes es 4-uniforme, asi que tiene una probabilidad diferencial máxima de $\frac{4}{2^8} = 2^{-6}$
  - Asi, la probabilidad diferencial total es de a lo sumo $(2^{-6})^{25} = 2^{-150}$
- Consecuencia del Teorema: Para poder montar un ataque DC con alguna probabilidad de éxito contra 4 rondas de Rijndael, se deben disponer de al menos 2^{150} mensajes de 1 bloque.
- Esos deben ser mensajes de 128 bits, el tamaño del bloque.

Resistencia de AES contra DC

- Prueba del Teorema:
  - En cualquier ataque diferencial, por el lema de Rijmen y Daemen, debe haber al menos 25 S-boxes con diferencias de entrada no nulas en 4 rondas.
  - Cada uno de esos S-boxes es 4-uniforme, asi que tiene una probabilidad diferencial máxima de $\frac{4}{2^8} = 2^{-6}$
  - Asi, la probabilidad diferencial total es de a lo sumo $(2^{-6})^{25} = 2^{-150}$
- Consecuencia del Teorema: Para poder montar un ataque DC con alguna probabilidad de éxito contra 4 rondas de Rijndael, se deben disponer de al menos 2^{150} mensajes de 1 bloque.
- Esos deben ser mensajes de 128 bits, el tamaño del bloque.
- Solo hay 2^{128} bloques de 128 bits, por lo tanto no es posible montar el ataque.

Linear Cryptanalísis

- Otro ataque que realiza un tipo distinto de aproximación lineal a los Sboxes es el ataque de de 1993 de Mitsuru Matsui llamado Criptoanálisis Lineal (LC)

Linear Cryptanalísis

- Otro ataque que realiza un tipo distinto de aproximación lineal a los Sboxes es el ataque de de 1993 de Mitsuru Matsui llamado Criptoanálisis Lineal (LC)
- No tenemos tiempo de explicarlo, pero resulta que el Sbox de Nyberg también es resistente en forma óptima contra este ataque, aunque la prueba es mucho mas complicada que en el caso DC.

Linear Cryptanalísis

- Otro ataque que realiza un tipo distinto de aproximación lineal a los Sboxes es el ataque de de 1993 de Mitsuru Matsui llamado Criptoanálisis Lineal (LC)
- No tenemos tiempo de explicarlo, pero resulta que el Sbox de Nyberg también es resistente en forma óptima contra este ataque, aunque la prueba es mucho mas complicada que en el caso DC.
- Asi que Rijndael también es resistente al LC