Class4crypt

Aula virtual de criptografía aplicada

Clase c4c4.4
Secreto perfecto y distancia de unicidad

Madrid, martes 8 de diciembre de 2020

Profesor Dr. Jorge Ramió A.

Temario de las clases Class4crypt

- Módulo 1: Principios básicos de la seguridad
- Módulo 2: Matemáticas discretas en la criptografía
- Módulo 3: Complejidad algorítmica en la criptografía
- Módulo 4: Teoría de la información en la criptografía 
- Módulo 5: Fundamentos de la criptografía
- Módulo 6: Algoritmos de criptografía clásica
- Módulo 7: Funciones hash en la criptografía
- Módulo 8: Criptografía simétrica en bloque
- Módulo 9: Criptografía simétrica en flujo
- Módulo 10: Criptografía asimétrica

Clases publicadas en Class4crypt (1/3)

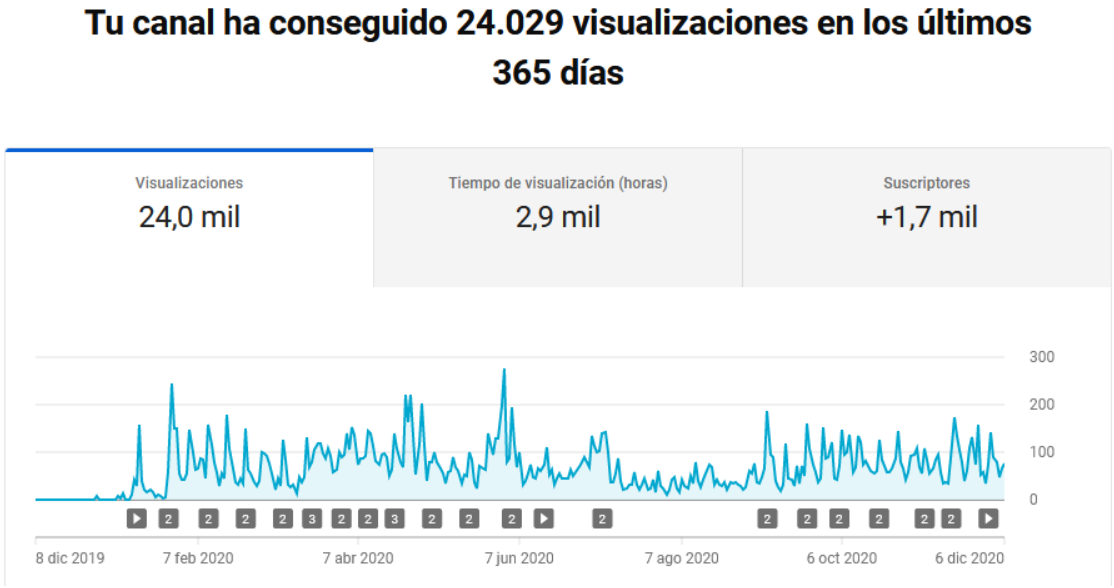
1. Presentación de Class4crypt
2. Ciberseguridad y criptografía
3. Algoritmo RSA
4. Operaciones modulares y conjunto de restos
5. Percepción de la inseguridad según las décadas
6. Criptografía asimétrica y la analogía de los candados
7. Protocolo de intercambio de clave de Diffie y Hellman
8. Ataque man in the middle al intercambio de clave de Diffie y Hellman
9. Cifrado por sustitución polialfabética: algoritmo de Vigenère
10. Criptoanálisis al cifrado de Vigenère por el método Kasiski
11. El homomorfismo de los enteros en la criptografía
12. Inverso aditivo, inverso xor e inverso multiplicativo
13. Cálculo de inversos con el algoritmo extendido de Euclides
14. Algoritmo de exponenciación modular rápida
15. Generación de claves RSA y estándar PKCS#1
16. Cifrado y descifrado con RSA parte 1
17. Cifrado y descifrado con RSA parte 2

Clases publicadas en Class4crypt (2/3)

18. Introducción a la criptografía moderna
19. Comparación entre cifra simétrica y cifra asimétrica
20. Fundamentos de la cifra simétrica en flujo
21. Registros de desplazamiento realimentados lineales y no lineales
22. Aleatoriedad en registros LFSR con polinomio primitivo
23. Fundamentos de la cifra simétrica en bloque
24. Algoritmo DES: redes de Feistel y cajas S
25. Algoritmo DES: expansión de clave, cifra y rellenos
26. ECB y CBC, modos de cifra con confidencialidad
27. CFB, OFB y CTR, modos de cifra con confidencialidad
28. Ataques al DES, DES Challenge y 3DES
29. Clasificación de los sistemas de cifra clásica
30. Vulnerabilidades de la información y amenazas
31. Seguridad informática vs seguridad de información
32. Tríada confidencialidad, integridad y disponibilidad
33. Raíces primitivas en un primo p
34. Fundamentos de complejidad algorítmica
35. El problema de la mochila
36. El problema del logaritmo discreto

Clases publicadas en Class4crypt (3/3)

37. El problema de la factorización entera
38. Cantidad de información e incertidumbre
39. Entropía de la información y codificador óptimo
40. Ratio y redundancia del lenguaje
41. Secreto perfecto y distancia de unicidad



¡COMENZAMOS!

Class4crypt c4c4.4

Módulo 4. Teoría de la información en la criptografía

Lección 4.4. Secreto perfecto y distancia de unicidad

1. Secreto de un sistema criptográfico
2. Cifrado con secreto perfecto
3. Cifrado sin secreto perfecto
4. Modelo de cifrador aleatorio
5. Distancia de unicidad

Secreto de un sistema criptográfico

- Shannon define el secreto de un criptosistema como la incertidumbre del mensaje en claro M conocido el criptograma C, en cuya cifra se ha usado una clave K
- Tenemos estos espacios: $M = \{M_1, M_2, \ldots M_n\}$, $C = \{C_1, C_2, \ldots C_n\}$, $K = \{K_1, K_2, \ldots K_n\}$
- Y en ellos se cumple que: $\Sigma\, p(M_i) = 1$, $\Sigma\, p(C_i) = 1$, $\Sigma\, p(K_i) = 1$
- Sea p(M) la probabilidad de enviar un mensaje M. Si tenemos n mensajes M_i equiprobables, entonces $p(M_i) = 1/n$
- Sea p(C) la probabilidad de recibir un criptograma C. Si cada uno de los n criptogramas C_i tienen igual probabilidad, entonces $p(C_i) = 1/n$
- Sea $p_M(C)$ la probabilidad de que a partir de un texto en claro M_i se obtenga un criptograma C_i
- Y sea $p_C(M)$ la probabilidad de que una vez recibido el criptograma C_i éste provenga de un texto en claro M_i

Cifrado con secreto perfecto (1/3)

Un sistema tiene secreto perfecto si el conocimiento del texto cifrado no nos proporciona ninguna información acerca del mensaje. Es decir, cuando la probabilidad de acierto al recibir el elemento i+1 es la misma que en el estado i

Secreto perfecto $\Rightarrow$ $p(M) = p_C(M)$

La probabilidad p de enviar un mensaje M con texto en claro p(M) o, en otras palabras, la probabilidad a priori, será igual a la probabilidad p de que una vez conocido un criptograma C, éste se corresponda a un mensaje M cifrado con la clave K. Esta última, ahora conocida como la probabilidad a posteriori, es $p_C(M)$

Cifrado con secreto perfecto (2/3)

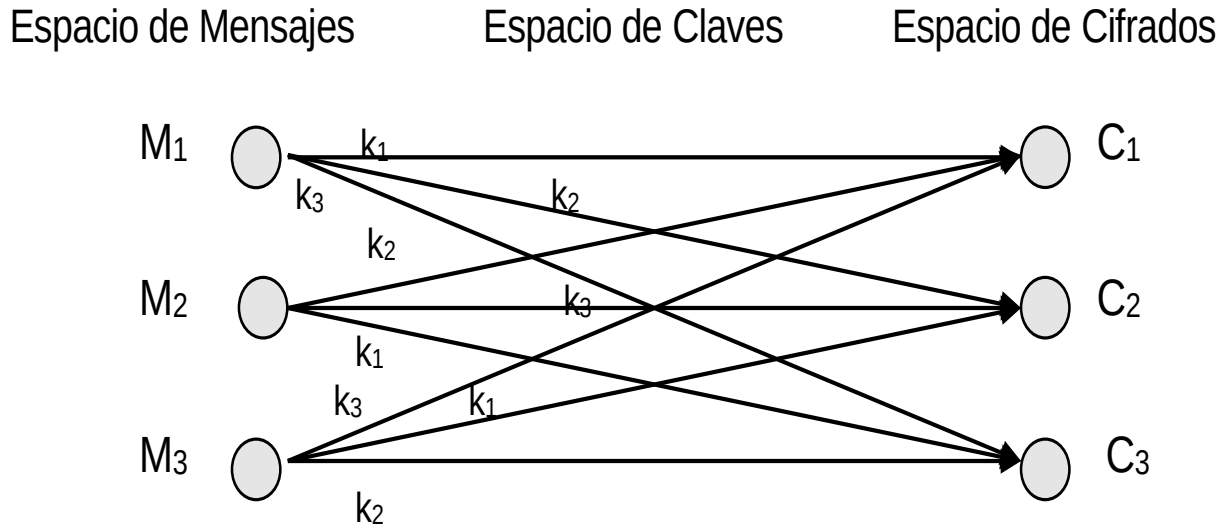
- La probabilidad p de cifrar un mensaje en claro M usando una clave K y que se convierta en un criptograma C será $p_M(C)$
- Luego, como M debe haberse cifrado con alguna clave K

$$p_M(C) = \sum_{k=1}^{k=n} p(K) \qquad \text{donde } C = E_K(M) \quad (E = \textit{encrypt}, \text{ con clave K})$$

- Es decir, deberá cumplirse que: $\exists\, k_j \,/\, E_{kj}(M_i) = C_i$
- Esto nos indica que, para lograr un secreto perfecto, el espacio de claves debe ser mayor o al menos de igual tamaño que el espacio de mensajes
- Algo en teoría imposible, excepto en el denominado cifrado de Vernam

Cifrado con secreto perfecto (3/3)

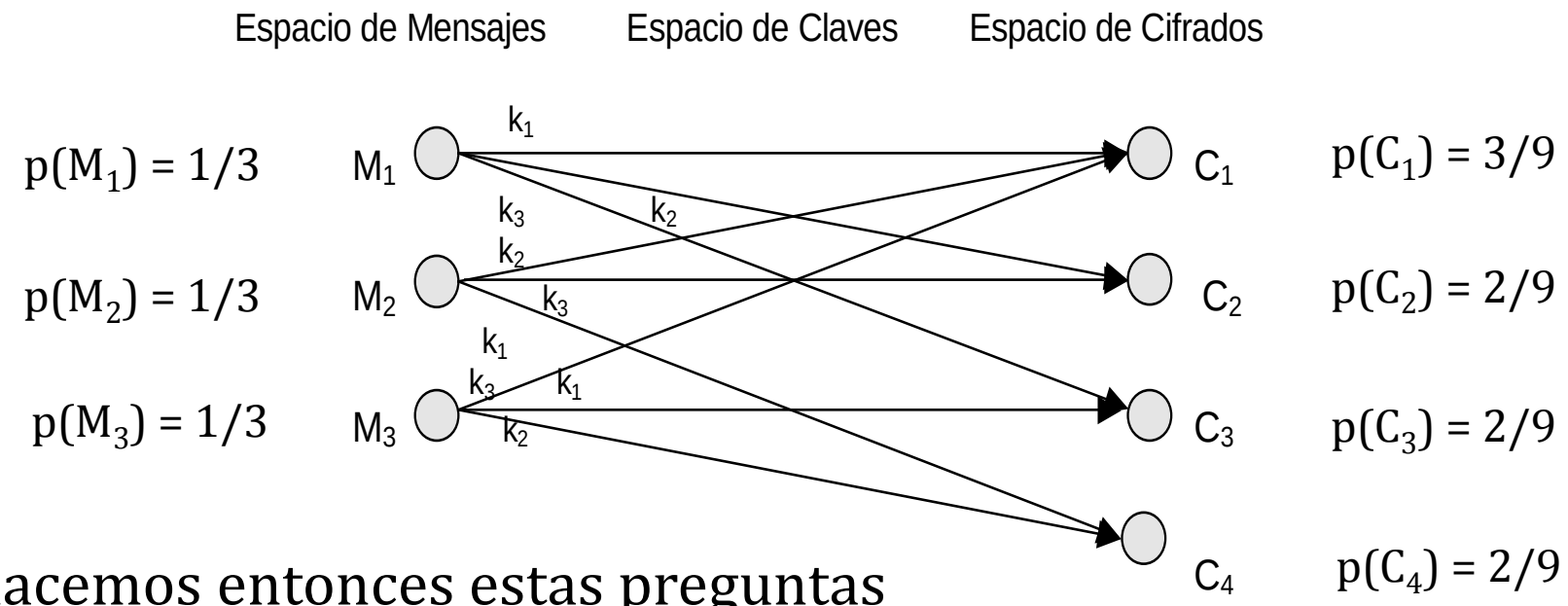
- La condición necesaria y suficiente del secreto perfecto es que para cualquier valor de mensaje M, se cumpla que la probabilidad de recibir el criptograma C, resultado de la cifra de M con una clave K, sea la misma que recibir ese mismo criptograma C, resultado ahora de la cifra de un mensaje M' cifrado con una clave K'
- Es decir, $p_M(C) = p(C)$ para todo valor de M



$p(M) = 1/3$ $p(C) = 1/3$

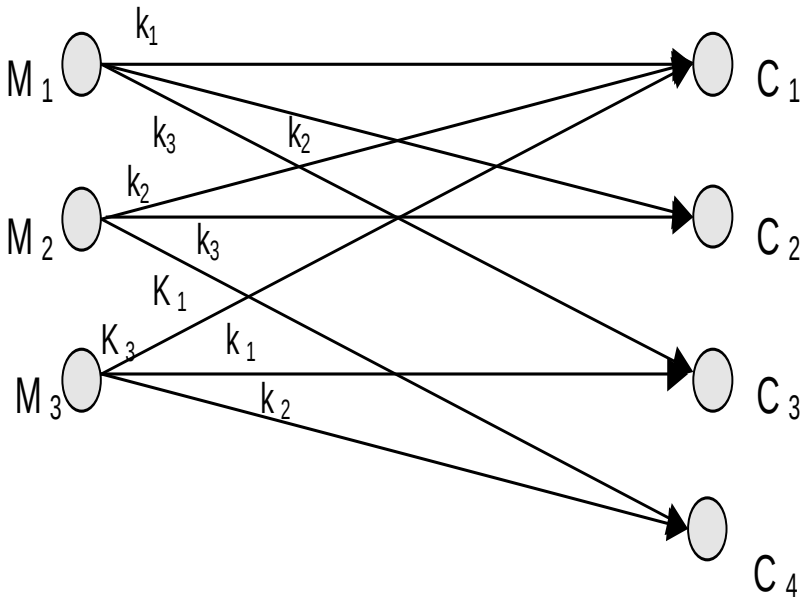
$p_M(C) = 1/3$ $p_C(M) = 1/3$

Cifrado sin secreto perfecto (1/2)



- Nos hacemos entonces estas preguntas
- ¿Cuál es la probabilidad de que un mensaje M_i cifrado con una clave K se convierta en un criptograma C_i, es decir $[P_{Mi}(C_i)]$, y la de que un criptograma C_i sea el resultado de la cifra de un mensaje M_i con clave K, es decir $[P_{Ci}(M_i)]$?

Cifrado sin secreto perfecto (2/2)



$P_{C1}(M_1) = 1/3$	$P_{C1}(M_2) = 1/3$	$P_{C1}(M_3) = 1/3$
$P_{C2}(M_1) = 1/2$	$P_{C2}(M_2) = 1/2$	$P_{C2}(M_3) = 0$
$P_{C3}(M_1) = 1/2$	$P_{C3}(M_2) = 0$	$P_{C3}(M_3) = 1/2$
$P_{C4}(M_1) = 0$	$P_{C4}(M_2) = 1/2$	$P_{C4}(M_3) = 1/2$

$p_{M1}(C_1) = 1/3$	$p_{M1}(C_2) = 1/3$	$p_{M1}(C_3) = 1/3$	$p_{M1}(C_4) = 0$
$p_{M2}(C_1) = 1/3$	$p_{M2}(C_2) = 1/3$	$p_{M2}(C_3) = 0$	$p_{M2}(C_4) = 1/3$
$p_{M3}(C_1) = 1/3$	$p_{M3}(C_2) = 0$	$p_{M3}(C_3) = 1/3$	$p_{M3}(C_4) = 1/3$

Definición de distancia de unicidad

- Se entenderá por distancia de unicidad a la cantidad de N letras en el texto cifrado o criptograma, mínima necesaria para que se pueda intentar con ciertas expectativas de éxito un criptoanálisis para romper la clave
- Este valor se obtiene cuando la equivocación de esa clave $H_C(K)$, o entropía condicional de la clave, se acerca a cero o tiende a anularse
- Dada la redundancia del lenguaje, a medida que se tenga un criptograma más largo la tarea de ataque del criptoanalista se va reduciendo
- Esto porque el atacante puede confiar más en los resultados que obtiene al aplicar las estadísticas y características del lenguaje sobre el criptograma
- Se buscará entonces el tamaño mínimo de N letras del criptograma que permita esperar que la solución de la clave K buscada sea única
- Para ello, se supondrá un esquema de cifrador aleatorio como el que se describe en las diapositivas siguientes

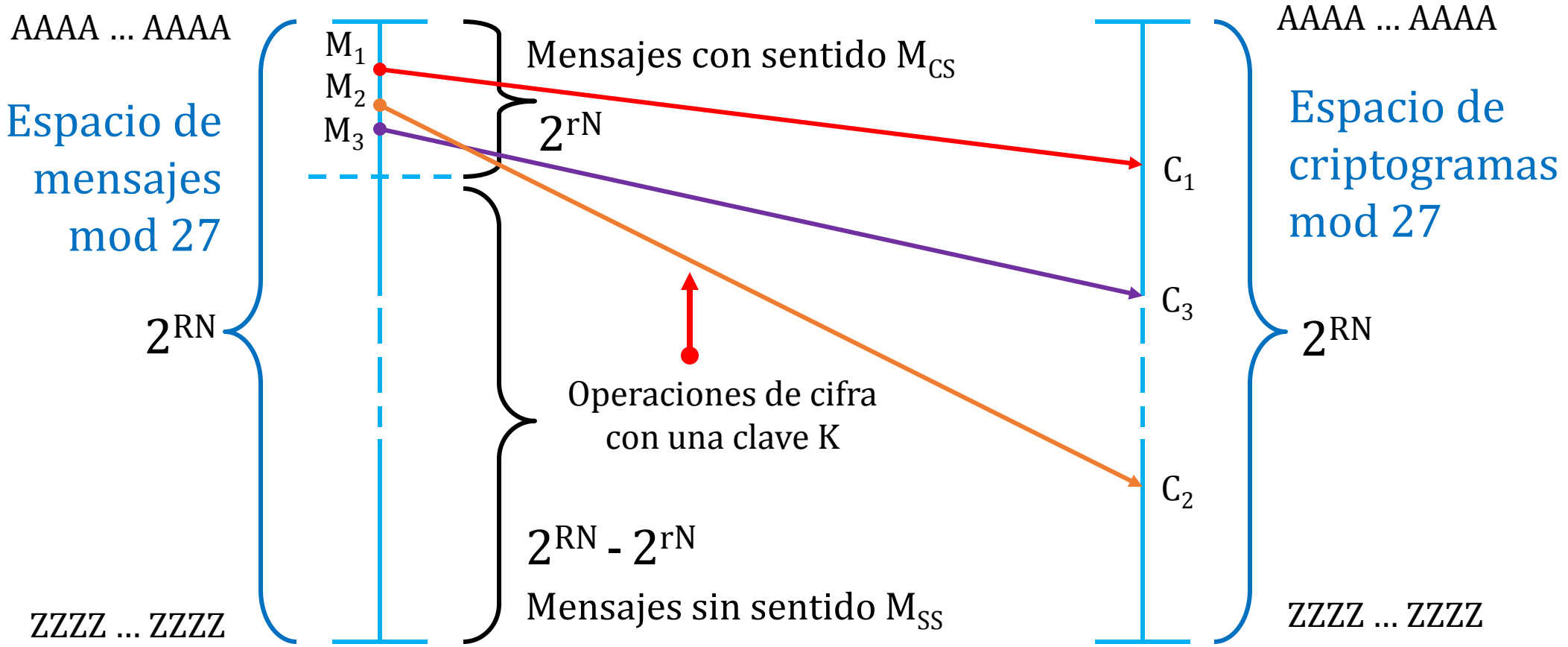
Parámetros del cifrador aleatorio (1/2)

- Existirán 2^{RN} mensajes posibles de longitud N
- Existirán 2^{rN} mensajes de longitud N con sentido
- El espacio de mensajes de longitud N se dividirá en:
  - Espacio de los mensajes con sentido: $M_{CS} = 2^{rN}$
  - Espacio de los mensajes sin sentido: $M_{SS} = 2^{RN} - 2^{rN}$
- En este escenario, los 2^{rN} mensajes con sentido M_{CS} van a ser equiprobables, siendo esta probabilidad $p(M_{CS}) = 1/2^{rN} = 2^{-rN}$
- El resto ($2^{RN} - 2^{rN}$) son mensajes sin sentido M_{SS}, no generados porque hablamos de texto, con una probabilidad nula $p(M_{SS}) = 0$

Parámetros del cifrador aleatorio (2/2)

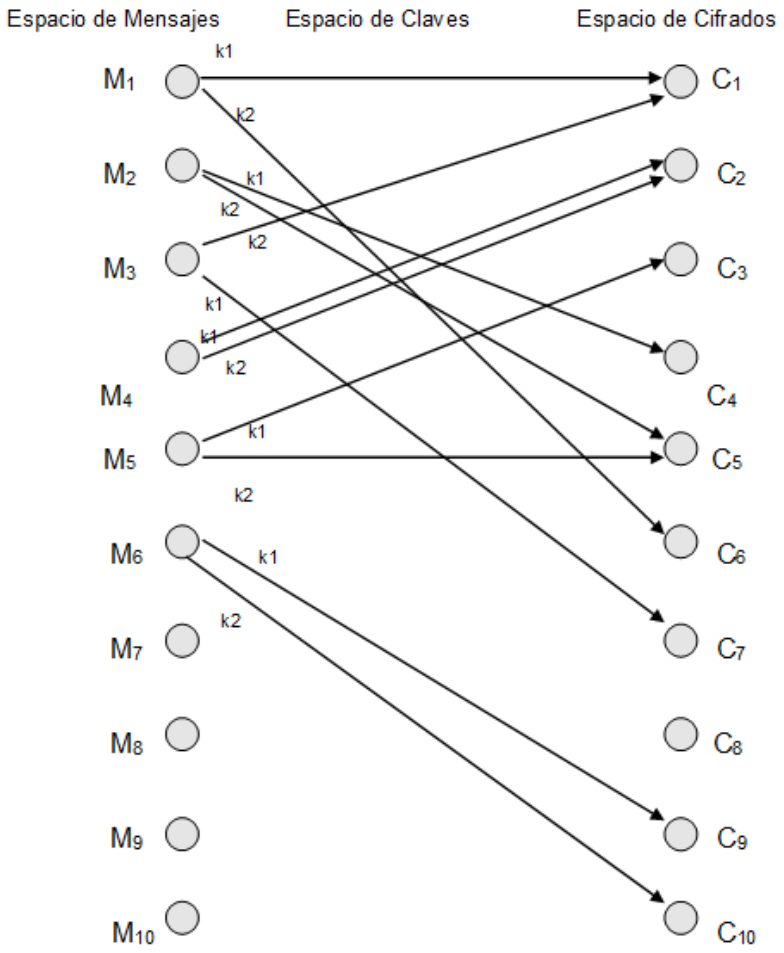
- Además, existirán $2^{H(K)}$ claves equiprobables
- En donde H(K) es la entropía de la clave
- Cada una de ellas con una probabilidad $p(K) = 1/2^{H(K)} = 2^{-H(K)}$
- Con cada una de estas claves se cifrarán todos los mensajes con sentido M_{CS}, dando lugar a 2^{RN} criptogramas posibles C con una longitud N
- A diferencia de los mensajes, como es lógico los criptogramas C obtenidos serán todos equiprobables, todos son "sin sentido"
- Con estos datos se obtiene el esquema de un cifrador aleatorio que se muestra en la siguiente diapositiva

Cifrador aleatorio mensajes de longitud N



Veamos los escenarios de este modelo de cifra para sólo dos claves: k_1 y k_2

Escenarios cifrador aleatorio para k_1 y k_2



- Una solución verdadera SV, será aquella en la que un criptograma está asociado sólo a un texto en claro con sentido y que ha sido cifrado con una única clave k_i
- Una solución falsa SF será cualquier otro resultado de cifra diferente al anterior
- Soluciones verdaderas SV en el esquema mostrado
  - $C_3 = E_{k1}(M_5)$ $C_4 = E_{k1}(M_2)$ $C_6 = E_{k2}(M_1)$ $C_7 = E_{k1}(M_3)$
  - $C_9 = E_{k1}(M_6)$ $C_{10} = E_{k2}(M_6)$
- Soluciones falsas SF en el esquema mostrado
  - $C_2 = E_{k1}(M_4)$ $C_2 = E_{k2}(M_4)$ $C_5 = E_{k2}(M_2)$ $C_5 = E_{k2}(M_5)$
  - $C_1 = E_{k1}(M_1)$ $C_1 = E_{k2}(M_3)$

1. Una solución falsa SF <u>obvia</u> será la del criptograma C_2
2. Una solución falsa SF <u>débil</u> será la del criptograma C_5
3. Una solución falsa SF <u>fuerte</u> será la del criptograma C_1

Cálculo de la distancia de unicidad (1/2)

- Para cada solución verdadera SV de un texto M cifrado con una clave k del espacio de claves $2^{H(K)}$, existirán otras $(2^{H(K)} - 1)$ claves con la misma probabilidad de entregar una solución falsa SF
- Sea q la probabilidad de obtener un mensaje con sentido M_{CS} al descifrar (o criptoanalizar) un criptograma C
- $q = 2^{rN}/2^{RN} = 2^{(r - R)N} = 2^{-DN}$ (Redundancia $D \approx 3{,}4$ en módulo 27)
- Luego, $SF = (2^{H(K)} - 1)\ q = (2^{H(K)} - 1)\ 2^{-DN} = 2^{H(K) - DN} - 2^{-DN}$
- Si 2^{-DN} puede despreciarse por pequeño, entonces $SF \approx 2^{H(K) - DN}$
  - O lo que es lo mismo, $H(K) - DN = \log_2 SF$

Cálculo de la distancia de unicidad (2/2)

- La solución SF = $2^{H(K) - DN} = 0$ es imposible porque sólo se llegaría a ella de forma asintótica y con un valor de N infinito
- Se aceptará entonces que haya como máximo una sola solución falsa SF y, por tanto, nos acercamos a la solución única
- Si SF = $2^{H(K) - DN} = 1$, entonces $H(K) - DN = 0$
- Por lo tanto $N = H(K)/D$ será la distancia de unicidad
- Este valor es sólo de referencia para comparar los diferentes sistemas de cifra clásica. Para romper una cifra será necesario contar al menos con un tamaño de criptograma 10 veces mayor a N, siendo habitual una cantidad mucho mayor de texto cifrado

Conclusiones de la Lección 4.4

- Shannon define el secreto de un sistema de cifra como la incertidumbre del mensaje en claro M conocido el criptograma C
- Tanto los mensajes M, como las claves K y los criptogramas C tendrán una probabilidad p asociada y tendrán, además, su correspondiente espacio
- Un sistema tiene secreto perfecto si el conocimiento del texto cifrado no proporciona ninguna información acerca del mensaje. Se logra si el espacio de claves es al menos de igual tamaño que el espacio de mensajes
- La distancia de unicidad es la cantidad de N letras del criptograma mínima necesaria para intentar un criptoanálisis con ciertas expectativas de éxito
- Definiendo un esquema de cifrador aleatorio, se llega a que esa distancia de unicidad (un indicador sólo para comparación) viene dada por H(X)/D

Un proyecto sin ánimo de lucro

- Class4crypt es un proyecto sin ánimo de lucro
- Si te ha gustado el vídeo, has aprendido algo nuevo o bien has podido reforzar algún conocimiento que ya tenías
- Entonces, por favor, pon un "**Me gusta**" al vídeo
- Si deseas expresar alguna opinión sobre el contenido de esta clase o tienes alguna duda, hazlo por favor en YouTube. Todos los comentarios serán muy bien recibidos y las dudas que plantees serán contestadas a la mayor brevedad posible

¡Muchas gracias!

Lectura recomendada

Fin de la clase 4.4

- Communication Theory of Secrecy Systems, C. E. Shannon, The Bell System Technical Journal, Vol. 28, 1949
  - https://www.cs.virginia.edu/~evans/greatworks/shannon1949.pdf
- Distancia de unicidad
  - https://es.wikipedia.org/wiki/Distancia_de_unicidad
- Shannon's Theory of Secrecy Systems, Eli Biham - May 3, 2005 (diapositivas de clase)
  - http://www.cs.technion.ac.il/~cs236506/04/slides/crypto-slides-02-shannon.2x2.pdf
- Criptografía y Seguridad en Computadores, Capítulo 3 Teoría de la información, Manuel Lucena, versión 5-0.1.4, noviembre 2019
  - http://criptografiayseguridad.blogspot.com/p/criptografia-y-seguridad-en.html

Más lecciones en el canal Class4crypt

Fuera webcam y dentro música

SUSCRIBIRSE

1.750 suscriptores
8 diciembre 2020

- https://www.youtube.com/user/jorgeramio

Licencia y créditos

- Estas videoclases y la documentación utilizada en ellas están publicadas bajo licencia *Creative Commons* tipo CC BY-NC-ND 4.0
  - Reconocimiento - No Comercial - Sin Obra Derivada

- Esto permite que otros puedan descargar esta obra y compartirla con otras personas, siempre que se reconozca su autoría, pero no se puede cambiar de ninguna manera su contenido ni se puede utilizar comercialmente

- Música:
  - Enter_Blonde, Max Surla, Media Right Productions, YouTube Audio Library - Free Music https://www.youtube.com/audiolibrary/music?nv=1

La próxima semana,
última clase de este
cuarto módulo y ...
¡una sorpresa!

Criptosaludos