Ciencia Latina
Revista Multidisciplinar

DOI: https://doi.org/10.37811/cl_rcm.v6i3.2259

El contenido efímero aplicado en la seguridad de la información

Alan Rodrigo Corini Guarachi
alan_corini_g@hotmail.com
Universidad Nacional Siglo XX
La Paz - Bolivia

RESUMEN

Existe un antes y un después de Snapchat, las publicaciones que expiran en 24 horas a partir de la publicación revolucionó los medios sociales, empezando con las campañas publicitarias de películas en Snapchat o en diferentes medios sociales como Facebook, Twitter, Instagram, haciendo que las empresas aprovecharan estas plataformas, esta metodología se puede usar para la seguridad de la información protegiendo la información por un tiempo limitado, por ejemplo series de televisión, películas, en los últimos años hubo filtraciones que costaron millones de dólares a las empresas productoras, el contenido efímero tendrá que ser compatible con cualquier algoritmo existente como ser AES, 3DES, RSA entre otros, solo se tomara en cuenta la clave de cifrado, que cambiara aleatoriamente hasta que se cumpla el tiempo de protección, de esta manera se asegurara que la información se publicada en el tiempo estimado.

Este modelo puede garantizar la protección de la información incluso si se utiliza una contraseña insegura, esto se debe a la generación de combinaciones aleatorias que son utilizadas en cada ejecución del algoritmo

Palabras clave: *snapchat; seguridad; cifrado; contenido efímero; descifrado; combinaciones aleatorias.*

Correspondencia: alan_corini_g@hotmail.com
Artículo recibido: 20 abril 2022. Aceptado para publicación: 05 mayo 2022.
Conflictos de Interés: Ninguna que declarar

Como citar: Corini Guarachi, A. R. (2022). El contenido efímero aplicado en la seguridad de la información. Científica Multidisciplinar, 6(3), 792-805. DOI: https://doi.org/10.37811/cl_rcm.v6i3.2259

Ephemeral content applied to information security

ABSTRACT

There exists a before and after within Snapchat. The publication which expires 24 hours after being posted revolutionized social media. This began with publicity campaigns for movies in Snapchat and other social media sites like Facebook, Twitter, and Instagram. This caused businesses to take advantage of these platforms. This methodology can be used for information security, protecting it for a limited time. For example, Television Series and Movies which were leaked in the last few years have cost production companies millions dollars. The ephemeral content must be compatible with any existing algorithms such as AES, 3DES, RSA, and others. Only the encryption code is taken into account, which changes randomly until the designated time of protection is fulfilled. In this way they assure that the information is only published for the determined time. This model can guarantee the protection of information even if an insecure password is used. This is because of the generation of random combinations, which are used every time the algorithm is called upon.

Keywords: *snapchat; security; encryption; ephemeral content; decryption; random combinations.*

1. INTRODUCCIÓN

La fecha de caducidad puede ser aplicado en información que estará disponible en cuestión de horas o días, esta característica se observa inversamente en diferentes aplicaciones móviles como Facebook, WhatsApp, Instagram, Snapchat entre otros, se publica el contenido por un cierto tiempo determinado y se autodestruye al concluir.

En varias ocasiones empresas reportaron sustracción de contenido digital que sería estrenado en los próximos días, por ejemplo, la serie de televisión Juego de Tronos o la película Piratas del Caribe V “La venganza de Salazar”.

En el contexto nacional se puede aplicar al momento de presentación de propuestas, comunicados, cortes programados o cualquier otro procedimiento que puede ser publicado en poco tiempo.

1.1 Antecedentes

Cada cierto tiempo se produce filtraciones de series de televisión o películas causando pérdidas calculadas en millones de dólares a las empresas productoras

1.2 Snapchat

Es una red social que opera de manera distinta a las demás, Snapchat corta con la idea de la permanencia, con el concepto del favorito o del "me gusta" y con el medidor de popularidad que se ve reflejado en el número de seguidores. Nadie sabe cuántos ven tus publicaciones y nadie sabe a quiénes sigues, excepto tú. Los videos y fotos publicados solo ponen en evidencia a sus usuarios durante 24 horas. Pasado un día, lo que se publicó en la APP desaparece del historial y los mensajes que se envían por chat se auto destruyen tan pronto son leídos por quien los recibe. (De la Pava, 2016)

Actualmente Snapchat cuenta 186 millones de usuarios diarios más que Twitter (York, 2019)

1.3 Whatsapp Y Facebook

En el año 2017 WhatsApp implementó en su aplicación los estados, una característica propia de Snapchat, y pronto lo acompañaría otras aplicaciones como ser Facebook, Instagram y Facebook Messenger. Varios medios digitales retrataron esta opción como una copia de la tecnología implementada por Snapchat.

Forbes se refirió a esta función como una "actualización radical" que "va a cambiarlo todo" convirtiendo la mensajería "por primera vez" en una "plataforma para

consumir el contenido de una manera pasiva" como hace ahora la gente cuando navega por los estados en Facebook o Instagram. Según esta función, el estado publicado estará disponible para la lista seleccionada de contactos durante 24 horas, después de lo cual desaparecerá de forma automática, algo que Snapchat introdujo en su función Stories ('Historias') hace tres años, lo que llegó a ser todo un éxito. (RT Sepa Más, 2017)

1.4 El Arte de esconder a simple vista

Esconderse a simple vista puede ser algo muy útil, se puede usar en muchos casos, pero la persona que sabe el secreto es la única que puede entenderlo, por ejemplo, tenemos los siguientes casos:

- Ocultar la llave de ingreso de su domicilio debajo de una planta o en el hueco de un ladrillo de la pared.
- Ocultar el código de la alarma en el collar de la mascota.

En todos estos ejemplos una persona sabe el secreto, sabe el significado, otro individuo lo puede descubrir, pero puede demorar un tiempo razonable.

1.5 El Impacto del contenido efímero

Desde que apareció Snapchat, empezó a revolucionar el contenido que se publica en las redes sociales, con su mágico ascenso, varias empresas o artistas empezaron a publicar contenido en la nueva red social de Snapchat, el primero fue el anuncio de pago de la película Ouija de Universal Pictures, también habilitaron los filtros, que revoluciono en esos años, varias empresas empezaron a copiar la idea, en el ámbito académico muchos investigadores empezaron a clasificar este fenómeno como de gran impacto en medios sociales. El valor del contenido está precisamente en su fugacidad, ese tiempo limitado con el que cuenta. (Rubio & Perlado, 2017)

A partir de este hecho varias compañías imitaron esta opción como estrategia en los medios sociales, lo catalogan como contenido efímero.

El contenido efímero es aquel que dura un tiempo limitado y después se elimina de manera permanente. Puede utilizarse en distintos formatos de contenido ya sea vídeo, texto o imágenes. Subir contenido efímero aporta numerosos beneficios ya que a través de él podremos llegar a multitud de consumidores. (Carrillo, 2018)

El principal atractivo de este tipo de historias es que, como desaparecen, se genera una especie de necesidad imperiosa de verlo en ese instante, lo efímero agrega un toque emocionante y nos aleja de la necesidad de perfección. (Maldon.es, s.f.)

El "fast content", contenido rápido y efímero, se está popularizando a una velocidad vertiginosa, dando el salto a que los anunciantes lo aprovechen para llegar a un mayor número de consumidores mediante estos micro-momentos. (Símbolo Ingenio Creativo, 2019)

2. MATERIALES Y MÉTODOS

Se debe observar el factor de comunicación humana, se compone del envió, transmisión y recepción, un mensaje por un medio digital cumple con lo mencionado, tomando en cuenta él envió de un SMS, inicia en el dispositivo móvil, se escribe el mensaje, antes de enviar se cifra el contenido del mensaje, se transmite por la red del operador de telefonía móvil, el dispositivo recibe el mensaje, se descifra y el receptor puede leer el mensaje, el mensaje puede ser un comunicado, informes, promociones empresariales entre otros.

Las empresas de antivirus alertan sobre el mal uso o riesgos a la privacidad, ESET expone 5 riesgos más comunes como la manipulación de la información por terceros. (Gutiérrez, 2014)

Existen riesgos y debemos protegernos, como objetivo principal es proteger la información de diferentes ataques informáticos.

Se aplico los conceptos de la seguridad informática, para proteger la información se deberá diseñar un modelo que cumpla con las principales características de integridad, confidencialidad y disponibilidad.

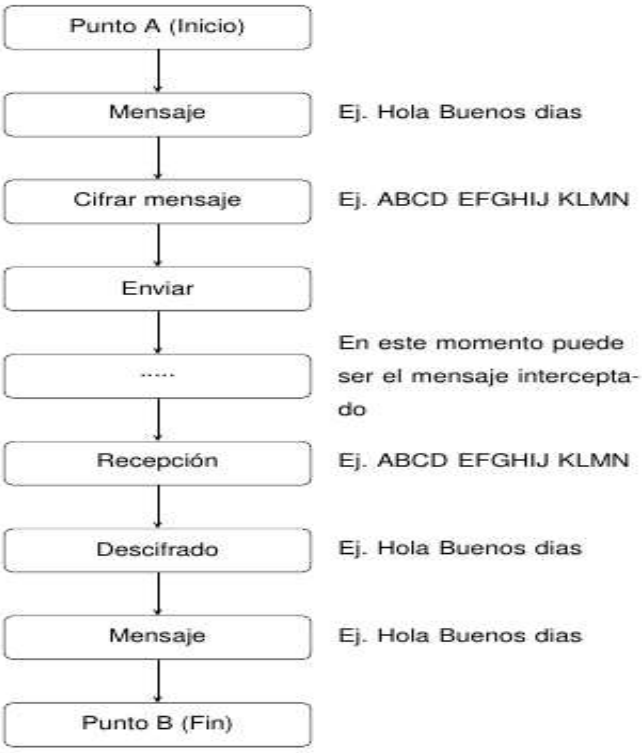
2.1 Seguridad de lo efímero

La seguridad de lo efímero, este principio nace con la tendencia de "contenido efímero", pero aplicado a la información que tiene que ser publicada en un periodo de tiempo, asemejándose a la tendencia que se implementó en las redes sociales, ¿se podría aplicar a la seguridad?.

Pero este modelo sería un inverso al uso tradicional. Por lo general se transmite una información de un punto A, hasta un punto B, con un mensaje oculto.

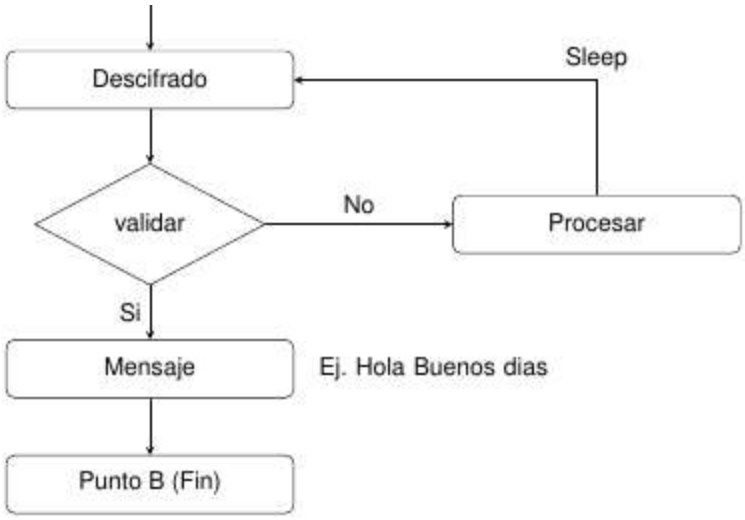
Actualmente se envía mensajes de la siguiente manera:

Figura 1. *Ejemplo básico de la transmisión de la información. Elaboración propia.*



La aplicación del contenido efímero tendrá que ser aplicado en el descifrado del mensaje, haciendo una modificación a la figura 1:

Figura 2. *Ejemplo de descifrado de mensaje. Elaboración propia.*



En la figura 2, se garantizará que se cumpla el tiempo estimado, pero dependiendo de cada equipo, se deberá tomar en cuenta los siguientes requerimientos:

- Generación de códigos aleatorios en cada combinación.
- Cifrado en forma escalonada.
- Tiempo de procesamiento
- Tiempo de espera

Códigos aleatorios. - La generación de códigos aleatorios permitirá que la clave inicial no sea la misma que se ejecuta en un paso anterior o siguiente, pero deberá volver a la clave inicial en una iteración por ejemplo se tiene las siguientes combinaciones:

Tabla 1. *Ejemplo de generación de códigos aleatorios. Elaboración propia*.

No.	Código
1	ab ∗ def c23416 ∗ ∗5∗
2	ab ∗ def c24163 ∗ ∗5∗
3	3b2d ∗ ∗ec1f 46 ∗ ∗5a
4	3b2dc ∗ ∗e1f 46 ∗ ∗5a
...	…….
99	∗b ∗ daef c24163 ∗ 5∗
100	ab ∗ d2ef c3416 ∗ ∗5∗

Cifrado en forma escalonada

Con la tabla 1, se puede suponer que el cifrado estará desde el número 1 hasta el número 100, para descifrar la información se tiene que utilizar la combinación número 100 hasta llegar a la clave inicial, en sentido contrario.

Existen varios métodos para cifrar la información, desde los más básicos como DES, 3DES, AES, RSA, son los más utilizados, también es necesario utilizar las recomendaciones de seguridad de empresas de programas de antivirus.

Algoritmo DES es un cifrado simétrico de 64 bits, de los cuales se utilizan 9 bits se utilizan como paridad, desarrollado por IBM (Ecured, 2019).

El algoritmo DES se considera inseguro y se recomienda no utilizarlo desde el año 1999, porque es vulnerable a cripto-análisis diferencial, aunque es un modelo teórico se utilizó para la vulneración. (De Luz, 2010)

Algoritmo 3DES se basa en el algoritmo DES, que aplica una serie de operaciones básicas para convertir un texto en otro cifrado, empleando una clave criptográfica.

3DES es el algoritmo que hace triple cifrado del DES (by.com.es, 2017), también se lo conoce como algoritmo TDES. (Francois, 2008)

El algoritmo 3DES, está siendo reemplazado por otros algoritmos que son más robustos como ser el AES y RSA en todas sus versiones.

El algoritmo AES funciona alimentando una clave de cifrado, esencialmente una cadena de dígitos en el algoritmo de cifrado y realizando de una serie de operaciones matemáticas basadas en esa clave de cifrado. (Dunning, s.f.)

El algoritmo AES tiene muchas variaciones y se realizó una comparación en la conferencia de la Universidad de la Habana Cuba, el cual describe a todas las versiones del algoritmo AES con todas las combinaciones o permutación que tienen cada algoritmo derivado, concluye que el carácter dinámico de las modificaciones no garantiza por sí misma el aumento de la seguridad del algoritmo, además la transformación que modifica ShiftRows no mantiene la difusión lograda en AES, esta transformación solo logra aumentar cuatro veces la complejidad del ataque DFA contra el algoritmo, pero el ataque sigue siendo realizable, por tanto esta transformación no incrementa sustancialmente la protección contra este tipo de ataque. (Legon, 2015)

El algoritmo RSA utiliza dos claves que sirven para cifrar o autentificar, este algoritmo se basa en la dificultad que presenta la factorización de números grandes. Las claves pública y privada se calculan a partir de un número que se obtiene como producto de dos primos grandes. Un atacante que quiera recuperar un texto claro a partir del criptograma y de la clave pública, tiene que enfrentarse a dicho problema de factorización, los números primos grandes deben ser mínimo de 200 cifras, para romper un cifrado RSA, podemos probar varias vías. Aparte de factorizar, que ya sabemos que es un problema computacional intratable en un tiempo razonable, podríamos intentar calcular directamente, o probar por un ataque de fuerza bruta tratando de encontrar la clave privada, probando sistemáticamente con cada uno de los números posibles del espacio de claves. (Carmona & Escribano, 2015)

Generalmente para descifrar la información o romper la clave se utilizan los siguientes métodos:

- Ataque de fuerza bruta
- Ataque de diccionario

- Ataque algebraico

Aunque estos ataques son comunes para descifrar una contraseña, otros se basan en un modelo matemático como el ataque DFA.

Tiempo de procesamiento y tiempo de espera. – Song público en su libro "Computational Number Theory and Modern Cryptography" (Song, 2012), el tiempo estimado de procesamiento para el cifrado y descifrado, por ejemplo:

Figura 3. *Tiempo de procesamiento estimado de cifrado y descifrado. Tomado de (Song, 2012)*

$$n^2 \approx n^3$$

En la figura 3, el valor de n es el tamaño en bits, para cifrar el procesamiento estimado es n^2y para descifrar es n^3.

3. RESULTADOS Y DISCUSIÓN

Para evaluar el modelo se debe utilizar varias combinaciones de forma escalonada, para descifrar se deberá hacer el mismo procedimiento de manera inversa, por ejemplo, se tiene la siguiente imagen.

Figura 4. *Imagen de prueba para análisis.*

Elaboración propia.

El archivo tiene las siguientes características.

Tabla 3. *Características del archivo de la figura 4.*

Característica	Valor
Ruta o nombre del archivo	Caso1.jpg
Tamaño	306,4KiB(313726)
Tiempo	50 segundos
Clave	123456789

Elaboración propia.

En la tabla 3 se muestra una clave de cifrado vulnerable, pero se entiende por mejora, a la complejidad algorítmica del cifrado, como se mencionó anteriormente se tiene que generar códigos aleatorios, a partir de la tabla 3.

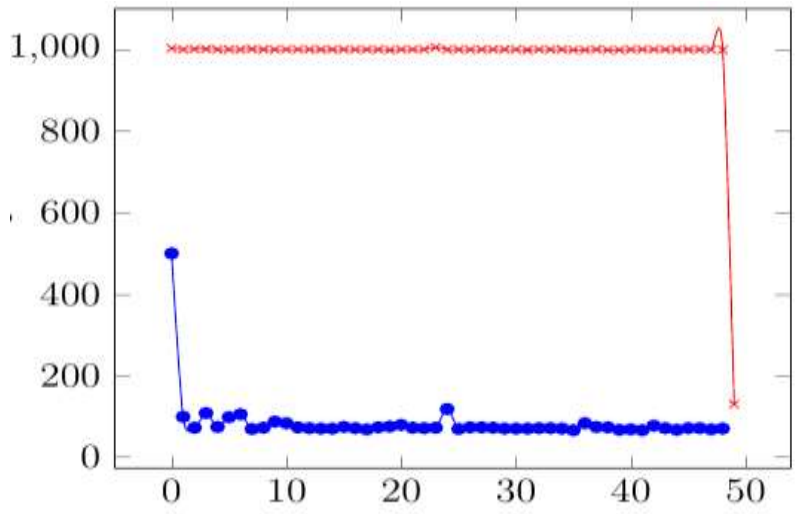
Tabla 4. *Códigos aleatorios de cifrado del archivo.*

No.	Código
1	123456789
2	423756189
3	234756189
4	239754618
...	.....
49	215678935
50	215674938

Elaboración propia.

Como es un cifrado escalonado, se cifró 50 veces, para descifrar se tiene que operar inversamente la tabla 4, empezamos con utilizar la clave “215674938”, luego “215678935”, hasta llegar a la primera clave “123456789”, aquí interviene el tiempo de espera y de procesamiento, después de hacer el descifrado de la figura 4, se tiene el siguiente detalle:

Figura 5. *Tiempo de procesamiento y espera del descifrado del archivo de la figura 4.*



Elaboración propia.

En la figura 5, tenemos dos ejes con valores de tiempo, en el eje X se tiene la duración y en el eje Y se tiene el procesamiento en milisegundos, la línea inferior de color azul es el tiempo de procesamiento y la línea roja es el proceso total en cada ejecución incluyendo el tiempo de espera o delay, este tiempo garantizara la ejecución del descifrado en el tiempo previsto, se puede observar que en cada iteración el proceso de descifrado varia, esto se debe a que cada clave es distinta y tiene su propio procesamiento de descifrado, esto también depende del procesamiento de la maquina anfitrión el tiempo de delay trata de corregir el espacio entre el tiempo de ejecución y el tiempo de procesamiento.

A todo esto, se obtiene los siguientes datos:

Tabla 5. *Resultados del procesamiento del cifrado y descifrado.*

	Cifrado (s)	Descifrado (s)
Tiempo inicial	2:25:20	2:27:22
Tiempo Final	2:25:24	2:28:11
Diferencia (s)	4	49

Elaboración propia.

Podemos concluir que el cifrado se completó en 4 segundos y para descifrar la información se demoró 49 segundos en procesar todas las combinaciones, se utilizó 50 combinaciones que partió de una clave insegura.

Para poder descifrar por un ataque de fuerza bruta, se deberá partir por descifrar la combinación No. 50 hasta llegar a la primera combinación, caso contrario la información no será descifrada.

3.1 DISCUSIÓN

En el presente trabajo se desarrolló el estudio inicial sobre el contenido efímero, se entiende por mejora a la complejidad del modelo que se utilizó para cifrar y descifrar la información de forma escalonada y permitir proteger su contenido por el tiempo que defina el usuario.

La presente propuesta explica un nuevo concepto de seguridad, basado en una característica de la red social Snapchat.

Existe documentación publicada por universidades, organismos gubernamentales, empresas de seguridad informática y antivirus sobre los riesgos que existe en la era tecnológica, pero existe poca información sobre el presente trabajo, de ahí nace la importancia de desarrollar en base a las características propuestas.

Aún hay mucho trabajo por mejorar la seguridad de la información a nivel nacional, proteger la información critica que se genera cada día, es importante reflexionar sobre el estado actual de los sistemas informáticos.

4. CONCLUSIÓN

A veces es bueno seguir la tendencia que se aplica en otras ramas de conocimiento, como se analizó primeramente el caso de Snapchat, el contenido efímero tiene un gran potencial para ser utilizado en diferentes sectores, desde los medios sociales, publicaciones programadas, entretenimiento, hasta ocultar o proteger la información antes de la fecha de publicación.

En el ejemplo se utilizó una clave muy vulnerable que puede ser fácilmente sometida a diferentes test de seguridad, pero la complejidad algorítmica de la generación de códigos aleatorios podría fortalecer la clave vulnerable, mientras más extenso sea el tiempo, más seguro podría ser el cifrado.

El cifrado efímero puede ser implementado con cualquier algoritmo de cifrado, simétrico o asimétrico, este procedimiento trabaja directamente con la clave a cifrar, indistintamente el método que se utilice, además este procedimiento permite integrar con los algoritmos AES, DES, 3DES y RSA.

Se tiene que probar con archivos de diferentes tamaños y extensiones, para probar la adaptabilidad del algoritmo y el tiempo de procesamiento que se utiliza.

Con la implementación de la Criptografía Cuántica y Blockchain para la protección de la información de entidades gubernamentales y privadas, la criptografía efímera se deberá adaptar o complementar a las tecnologías mencionadas, además se deberá regular a la normativa vigente de cada país.

5. LISTA DE REFERENCIAS

by.com.es. (27 de Enero de 2017). by.com.es. Recuperado el 14 de Marzo de 2019, de by.com.es: https://www.by.com.es/blog/algoritmos-encriptacion-aes-3des/

Carmona, L., & Escribano, C. (2015). *Departamento de Matemática Aplicada, Universidad Politécnica de Madrid*. Recuperado el 20 de Marzo de 2019, de Departamento de Matemática Aplicada, Universidad Politécnica de Madrid: http://www.dma.fi.upm.es/recursos/aplicaciones/matematica_discreta/web/aritmetica_modular/rsa.html

Carrillo, B. (1 de Abril de 2018). *Extravaganza communication*. Recuperado el 20 de Marzo de 2019, de Extravaganza communication: https://ec-global.es/blog/contenido-efimero-como-elemento-esencial-de-tu-estrategia-de-social-media/

De la Pava, B. (27 de Julio de 2016). *BBC Mundo*. Recuperado el 20 de Enero de 2018, de BBC Mundo: https://www.bbc.com/mundo/noticias-36895545

De Luz, S. (4 de Noviembre de 2010). *RedesZone*. Recuperado el 10 de Marzo de 2019, de RedesZone: https://www.redeszone.net/2010/11/04/criptografia-algoritmos-de-cifrado-de-clave-simetrica/

Dunning, D. (s.f.). *Techlandia*. Recuperado el 15 de Marzo de 2019, de Techlandia: https://techlandia.com/funciona-aes-info_215975/

Ecured. (14 de Marzo de 2019). *Ecured*. Obtenido de Ecured: https://www.ecured.cu/DES

Francois, J. (16 de Octubre de 2008). *es.ccm.net*. Recuperado el 20 de Marzo de 2019, de es.ccm.net: https://es.ccm.net/contents/130-introduccion-al-cifrado-mediante-des

Gutiérrez, C. (29 de Agosto de 2014). *welivesecurity*. Recuperado el 31 de Julio de 2019, de welivesecurity By Eset: https://www.welivesecurity.com/la-es/2014/08/29/top-5-riesgos-privacidad-debes-conocer/

Legon, C. (2015). COMPARISON OF DYNAMIC AES VARIANTS . Comparacion de variantes de AES Dinamico. *Universidad de las Ciencias Informaticas*. Recuperado el 19 de Marzo de 2019, de https://www.researchgate.net/publication/329755786_COMPARISON_OF_DYNAMIC_AES_VARIANTS_Comparacion_de_variantes_de_AES_Dinamico

Maldon.es. (s.f.). *MARKETING, DISEÑO Y TECNOLOGÍA PARA HACER CRECER EMPRESAS*. Recuperado el 19 de Marzo de 2019, de maldon.es: https://www.maldon.es/blog/ventajas-contenido-efimero/

RT Sepa Más. (21 de Febrero de 2017). *RT Sepa Más*. Recuperado el 15 de Marzo de 2019, de RT Sepa Más: https://actualidad.rt.com/actualidad/231646-whatsapp-lanzar-nueva-funcion-estatus

Rubio, J., & Perlado, M. (Septiembre de 2017). Snapchat o el impacto del contenido efímero. Revista TELOS. Fundación Telefónica. *TELOS. Fundación Telefónica.*, 1-9. doi:0213-084X

Símbolo Ingenio Creativo. (14 de Febrero de 2019). *Simbolizate Ingenio Creativo*. Recuperado el 25 de Marzo de 2019, de http://simbolizate.com: http://simbolizate.com/tag/contenido-efimero/

Song, Y. (2012). *Computational Number Theory and Modern Cryptography.* Wiley Edición. Recuperado el 18 de Marzo de 2019, de https://books.google.com.bo/books?hl=es&lr=&id=eLAV586iF-8C&oi=fnd&pg=PP8&dq=Computational+Number+Theory+and+Modern+Cryptography,+Song+Y.+Yan&ots=RCB5QRRqYN&sig=rgMbYVg4XAG0SYi7Rl7Lm3J5B4c#v=onepage&q=Computational%20Number%20Theory%20and%20Modern%20Crypt

York, P. (7 de Febrero de 2019). *Fayerwayer*. Recuperado el 15 de Marzo de 2019, de Fayerwayer: https://www.fayerwayer.com/2019/02/twitter-usuarios-diarios-activos/