COLOMBIA POTENCIA DE LA VIDA

TIC

Misión 2

Lección 2:

Algoritmos de cifrado moderno

TALENTO TECH | AZ PROYECTOS EDUCATIVOS | UTP Universidad Tecnológica de Pereira

Algoritmos de cifrado moderno

Tiempo de ejecución: 8 horas

Planteamiento de la sesión:

Debido a las vulnerabilidades de los algoritmos de cifrado clásicos, el auge de la computación, los algoritmos y la necesidad continua de seguir cifrando los datos, para poder enviar mensajes sin que otras personas diferentes a los destinatarios descifren el significado, surgieron metodologías más seguras para codificar mensajes. La seguridad de estos algoritmos se basa en cubrir las vulnerabilidades descritas en la lección 1.

Desarrollo de la sesión

Existen muchos algoritmos de cifrado que se desarrollaron con el fin de sobrepasar las vulnerabilidades que tenían los algoritmos clásicos. Sobre todo, en épocas en donde la ciencia y los métodos numéricos avanzaron a tal punto que el análisis criptográfico podía apoyar a investigadores en romper los códigos de cifrado de mensajes en ámbitos como la guerra y el espionaje. En esta unidad veremos algunos de ellos, así como algoritmos modernos computacionales empleados para proteger datos que deben ser compartidos en redes públicas como internet, en donde, cualquier persona puede leer los mensajes, pero solo un destinatario debe poder leer el contenido.

Preprocesamiento de los mensajes antes de ser cifrados

Una manera de mejorar los cifrados es preprocesar el texto a ser enviado, de eta manera se puede dificultar que un atacante (persona que no debe saber el mensaje) lo descifre por medio de técnicas de criptoanálisis. En el preprocesamiento se tienen técnicas como:

Conversión de alfabeto. En este caso se convierte el texto a un alfabeto diferente antes de ser codificado. Por ejemplo, algunos cifradores usan como alfabeto del texto plano el alfabeto latino. Si se desea cifrar un texto en español, es necesario realizar un proceso en cuyo resultado no aparezcan los caracteres H, J, Ñ, K, U, W y Y (por ejemplo, podrían sustituirse la U y la W por la V, la K con la Q, la Ñ por la N, la Y por la I, la J por la G, y eliminar la H).

Preproceso para dificultar el criptoanálisis. Consiste en técnicas que cambien la distribución de caracteres con el fin de que se dificulte el cripto análisis. Algunos ejemplos son:

- Incluir caracteres y fragmentos de texto que son para despistar y que no tienen ningún significado (caracteres nulos).

- Eliminar características que faciliten identificar el texto como el caso de signos de puntuación, espacios en blanco, tildes, entre otros. Esto evita que las ambigüedades un atacante las pueda resolver.

- Eliminar caracteres repetidos, como por ejemplo combinaciones RR o LL comunes en el español se suelen reemplazar por un carácter diferente para evitar poner en evidencia los textos.

- Conversión a números: Los caracteres se convierten a números antes de ser codificados.

Cifrados Clásicos por permutación

Estos métodos consisten en cambiar de lugar los elementos del mensaje a cifrar, logrando que el análisis criptográfico se dificulte y sea difícil para un atacante intentar descifrar el contenido del mensaje cifrado. Su funcionamiento es similar a la escítala (lección 1) en donde, al desenrollar el cuero de las varas el orden de los caracteres es alterado para que un mensaje no pueda leerse.
La manera más sencilla de crear un cifrado por transposición es cambiar las letras de lugar en un texto para que la lectura del mismo sea imposible.

Rail fence

Consiste en acomodar el texto a cifrar en una cuadrícula de tal forma que la permutación sea diferente al caso de la matriz en el ejercicio de la lección 1. Por ejemplo, si se quiere cifrar el texto “pasare por ti” este debe acomodarse en una cuadrícula que actuará como clave. El orden (ascendente o descendente) también es parte de la información que el destinatario debe conocer para descifrar el mensaje:

P						P					
	A				E		O				Ñ
		S		R				R		I	
			A						T		

En este caso el mensaje se ubica de forma descendente en una malla de 4 columnas haciendo un zigzag (o forma de ola). Nos aseguramos que el texto tenga olas completas, es decir que la cadena termine en la fila 2. Esto se logra rellenando con caracteres arbitrarios, como por ejemplo la letra Ñ. El texto cifrado resultará de leer las letras por columnas:

PPAEOÑSRRIAT

Para descifrar el texto se necesita calcular la longitud del texto y se requiere saber el numero de filas (o rieles). El número de caracteres por ola se calcula como:

Numero de caracteres por ola = (numero de rieles x 2) -2

En este caso daría (4x2)-2 = 6 caracteres por ola. El número de olas se obtiene como el número de caracteres dividido el número de elementos:

Numero de olas = num caracteres / num caracteres por ola

Numero de olas = 12 / 6 = 2

Luego se acomoda el texto en el formato de codificación. Sabemos que, hay que crear cuatro rieles, el mensaje tiene dos olas y cada ola va a contener seis elementos. El primer carácter del mensaje codificado será la cresta de la ola y el segundo carácter será la cresta de la segunda ola.

P						P					

Posteriormente se acomodan los caracteres separando cada uno en su ola correspondiente, sabiendo la forma que tiene cada ola (marcadas en color).

P						P					

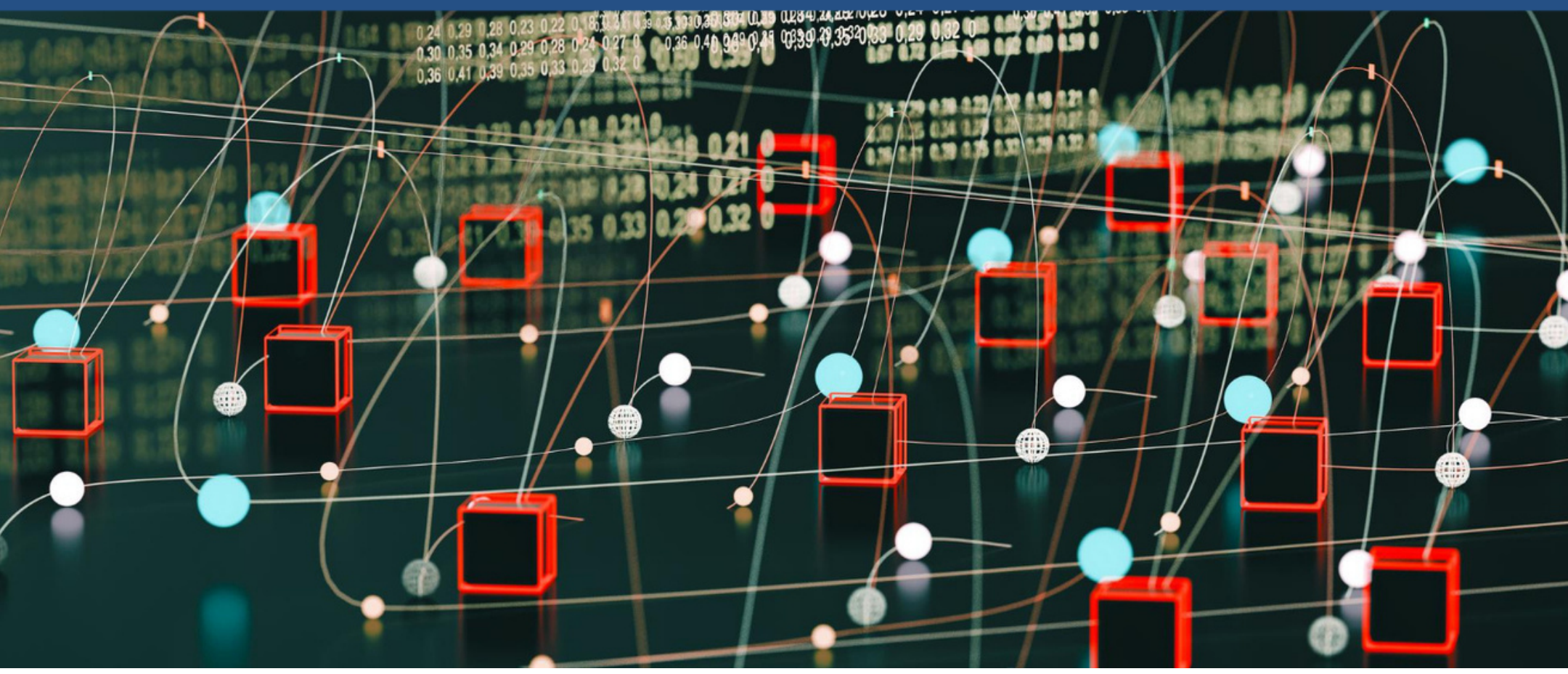
Luego se acomodan los caracteres por filas:

P						P					
	a				e		o				ñ

P						P					
	a				e		o				ñ
		s		r				r		i	

P						P					
	a				e		o				ñ
		s		r				r		i	
			a						t		

Finalmente se lee el mensaje desencriptado siguiendo la forma de las olas.



Cifrado por trasposición de grupos y series

Se logra agrupando el texto a cifrar en bloques de un cierto tamaño. Posteriormente se realiza una operación de permutación en grupos que se repiten periódicamente.

Ejemplo, se quiere emplear la permutación en grupos de 8 caracteres cuyo orden permutado será:

13572468

Es decir, se permutará el orden colocando primero la letras con posiciones impares y luego las letras con posiciones pares en los bloques de 8.

El texto a cifrar será: **Me gusta la criptografía**

Para cifrarlo tenemos que completar los grupos de 8 que hagan falta con caracteres arbitrarios.

1. Texto al que se le completan los bloques: **megustal acriptog rafiaxxx**
2. Se realiza la permutación de caracteres: **mgsaeutl arpocitg rfax aixx**

Finalmente se puede agrupar los caracteres en un número que evite que sea fácilmente decodificado, es decir, para no dar claves de que la permutación es en grupos de ocho, se puede presentar el mensaje todo pegado, o separado en grupos diferentes, por ejemplo, grupos de cinco: **mgsae utlar pocit grfax aixx**

En los algoritmos modernos, esta permutación se hace más difícil, reemplazando las permutaciones estáticas (13572468) por series matemáticas en donde, se requiere saber la serie para calcular las permutaciones en cada grupo, evidentemente las permutaciones van a ser diferentes en cada uno de los grupos. La ventaja de este método es que da una mayor fortaleza al cifrado. Por ejemplo, como serie se podría emplear los números primos, luego los números pares y finalmente los números sobrantes, por ejemplo:

1	2	3	4	5	6	7	8	9	10	11	12
M	E	N	S	A	J	E	F	I	N	A	L

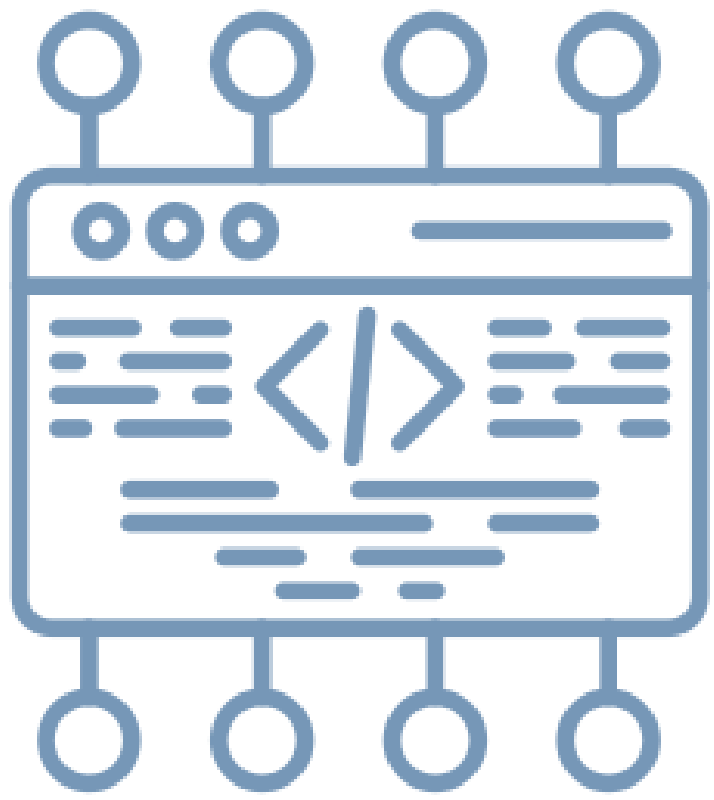
Empleando la serie descrita los números deberían ser ordenados como:

1, 2, 3, 5, 7, 11, 4, 6, 8, 10, 12, 9

En este caso los números en color verde son los primos, los rojos son los pares y en negro los números sobrantes.

El mensaje codificado será: **MENAA SJFNL I**

Ejercicio en clase:



Con los alumnos diseñar en Python funciones de cifrado por sustitución como las vistas en clase. Como actividad se propone que los estudiantes compartan datos cifrados entre ellos e intenten descubrir si es posible que una persona que no sea el destinatario se entere del contenido del mensaje.

Debata con los estudiantes cómo podría hacerse más complejo un cifrado mezclando técnicas vistas en la lección 1 y la lección 2.

Cifrado Delastelle

Este algoritmo se asejema al sistema monoalfabético del cuadrado de Políbio. Pero emplea una frase o un texto como método de codificación.

Para hacerlo se anotan las coordenadas de varias letras sin cifrar:

	A	B	C	D	E	F
A						
B						
C						
D						
E						
F						

Luego se emplea una frase, por ejemplo, tomar del libro El quijote de la mancha:

“En un lugar de la Mancha, de cuyo nombre no quiero acordarme, no ha mucho tiempo que vivía un hidalgo de los de lanza en astillero, adarga antigua, rocín flaco y galgo corredor.”

Posteriormente se acomodan las letras sobre la cuadrícula teniendo en cuenta de eliminar cualquier letra que ya se haya insertado en la cuadrícula. Para dificultar las cosas, se insertan números ascendentes en los lugares de la frase en donde hubiera espacios.

	A	B	C	D	E	F
A	E	N	1	U	2	L
B						
C						
D						
E						
F						

En este caso, la primera fila tiene el texto En un Lugar, pero la letra N no se emplea 2 veces, por lo que se salta a la siguiente palabra (lugar). Al saltar se aumenta el número que representa los espacios.

	A	B	C	D	E	F
A	E	N	1	U	2	L
B	G	A	R	3	D	4
C						
D						
E						
F						

Para la fila 2 se sigue la misma lógica, en este caso la palabra lugar no puede repetir la letra U ya que fue agregada previamente. De esta forma se sigue llenando la tabla:

	A	B	C	D	E	F
A	E	N	1	U	2	L
B	G	A	R	3	D	4
C	5	M	C	H	6	7
D	Y	O	8	B	9	0
E	Q/K	I	V	S	T	Z
F	F	J	Ñ	P	W	X

En el caso de la letra Q se suele juntar con la letra K, ya que encontrar textos que la contengan será difícil, por lo que puede ser agrupada. Apenas se acaben los números, se continúan escribiendo las letras del alfabeto, en orden de aparición del texto de referencia (el quijote).

Si queremos codificar el mensaje: “Este mensaje secreto” lo que hacemos es colocarlo en forma de tabla y realizar dos sustituciones, es decir, como si se tuviesen dos mensajes cifrados. El primer mensaje tendrá la columna correspondiente de la letra en la cuadrícula y el segundo mensaje tendrá la fila correspondiente en la cuadrícula. Como las filas y columnas son las letras de la A a la F, la salida será:

Para las columnas:

E	S	T	E	M	E	N	S	A	J	E	S	E	C	R	E	T	O
a	d	e	a	b	a	b	d	b	b	a	d	a	c	c	a	e	b

Para las filas:

E	S	T	E	M	E	N	S	A	J	E	S	E	C	R	E	T	O
a	d	e	a	b	a	b	d	b	b	a	d	a	c	c	a	e	b
a	e	e	a	c	a	a	e	b	f	a	e	a	c	b	a	e	d

Posteriormente se toman grupos de letras arbitrarios (por ejemplo grupos de 5)y se escriben los grupos de forma intercalada. Es decir, primero se ubican los cinco caracteres iniciales del mensaje cifrado por columnas, luego cinco caracteres del mensaje cifrado por filas y se repite hasta el final.

adeab aeeacabdbb aaebf adaccaeacb aeb aed

Finalmente se hace una sustitución. Para eso tomamos grupos de dos letras, dentro de los dos grupos de cinto intercalados. En este caso, los primeros dos grupos son la palabra: adeab-aeeac Utilizando cada pareja de caracteres como índices de la tabla, se sustituye cada par por el valor contenido. Es decir, la primera pareja es AD, con lo que, tomando la columna A y la fila D,en la tabla encontramos la letra Y. De la misma manera, las siguientes dos letras son EA, que corresponden al número 2. Luego, sigue BA que corresponde a la letra N. El mensaje codificado completo se muestra en última columna de la siguiente tabla.

E	S	T	E	M	E	N	S	A	J	E	S	E	C	R	E	T	O
a	d	e	a	b	a	b	d	b	b	a	d	a	c	c	a	e	b
a	e	e	a	c	a	a	e	b	f	a	e	a	c	b	a	e	d
Y	2	N	T	5	G	3	N	K	J	Y	5	1	2	R	Q	N	9

El mensaje será: **Y2N5G3NKJY512RQN9**

Para descifrar se requiere conocer el texto con el que se construyó la tabla y las reglas de agrupación de caracteres. En el ejemplo anterior se empleó una agrupación entre la letra Q y K.

Actividad:

Diseñe con los estudiantes mensajes y textos codificadores para el cifrado Delastelle. Luego, intercambien los mensajes con estudiantes y sigan las reglas para decodificarlos.

Cifrado trífido de Delastelle:

Este algoritmo es exactamente igual al cifrado bífido de Delastelle (visto anteriormente) solo que se emplea un cubo en lugar de una tabla. Es decir, los caracteres codificaran en tres coordenadas en lugar de dos. De esta forma se incrementa la complejidad del cifrado ya que los bloques tienen un orden diferente.

A pesar de la seguridad que tienen, un grupo de caracteres similares va a generar bloques similares. Al hacer análisis criptográficos es posible encontrar patrones que puedan ayudar a romper el cifrado.

Una forma de hacer mucho más seguro el cifrado es cambiando la matriz de caracteres antes del último paso de codificación. Con esto se tiene un algoritmo de matrices conjugadas.

Criptografía en la segunda guerra mundial

Durante la segunda guerra mundial, surgieron métodos para el envío de información cifrada por medio de los militares de los diferentes bandos. Si bien surgieron máquinas mecánicas y electromecánicas que permitían el cifrado de datos, muchos sistemas manuales se empleaban. También se desarrollaron técnicas de rotura de cifrados, como es el critpo análisis, en donde se estudiaban las debilidades de un sistema de cifrado para descifrarlo sin tener la información necesaria (clave o documentos generadores).

Se destacan métodos de cifrado con máquinas mecánicas alemanas como lo fue Enigma, que requirió de un avance considerable en el cripto análisis para romper el algoritmo de cifrado cuya clave cambiaba a diario. Destaca entre los analistas Alan Turing quien sería el fundador conceptual de la computación moderna.

Paralelo a estos sucesos, los ejércitos Esstadounidenses, en cooperación con los equipos de criptoanálisis Ingleses lograron romper algunos algoritmos criptográficos de los Japoneses, como es el caso del JN-25, y de la máquina Purpura.

Libretas de un solo uso

Este método de cifrado emplea una clave aleatoria anotada en una libreta la cual, era igual de larga que el texto a ser cifrado. La clave solo se podía emplear una vez, haciendo que el método de cifrado sea invulnerable. Este tipo de cifrado fue diseñado por Gilbert Vernam, y el uso de las libretas de un solo uso fue muy común a finales de la segunda guerra mundial. Gilbert Vernam también desarrolló un sistema de cifrado conocido como cifrado de Vernam, el cual es un cifrado de flujo. Es decir, conforme avanza el texto (fluye) se combina con la clave mediante operaciones matemáticas, creando una codificación pseudo aleatoria.

Cifrado Vernam

Este cifrado se desarrolló para encriptar textos a través de sustitución. El método consiste en emplear una llave para codificar el texto con la particularidad de que la llave sea tan larga como el texto.
Para encriptar un texto se asigna un número al texto plano en orden alfabético tanto para el texto como para la clave. Por ejemplo

- **Texto**: hijo
- **Clave:** casa

Reemplazando las letras por números, por ejemplo a=0, b=1… z=25.

Texto: 7 8 9 14 (en binario) : 0111 10001001 1110
Clave: 2 0 18 0 (en binario): 0010 0000 10010 0000

Posteriormente se ejecuta la función XOR bit a bit entre cada carácter del texto y cada carácter de la clave:

Resultado XOR: 0101 1000 11011 1110
Resultado en decimal: 5 8 27 14

A las letras que estén por encima de 26 le restamos 26 (para conservar el alfabeto)

Resultado en el alfabeto: 5 8 (27-26) 14

5 8 1 14

Convertimos de número a letra nuevamente con el sistema planteado (a=0, b=1…)

Texto cifrado: Fibo

Para descifrar se sigue el proceso a la inversa, a partir del texto cifrado se emplea la misma clave, se calculan las funciones XOR y se obtiene el texto sin codificar.

Ejercicio en clase: Empleando Python codifique con los alumnos una función que permita codifica y decodificar textos con el cifrado Vernam conociendo la clave.

El cifrado Vernam tiene varias ventajas:

1. Al ser del mismo largo la clave que el texto, la probabilidad de que una clave descifre es igual a cualquier cadena de valores de la misma longitud, por lo que sería muy complejo romper el cifrado.
2. No se pueden aplicar técnicas de reconocimiento de patrones ya que no hay pistas sobre letras repetidas ni frecuencias de caracteres.
3. El algoritmo es simple, permite rápidamente encriptar y desencriptar un texto solo con la operación XOR.

Sin embargo, tiene algunas desventajas como es el manejo de la clave, ya que, para que sea totalmente indescifrable, la clave debe ser un número aleatorio real del mismo largo del texto. Ya que la clave no se puede volver a emplear, crear y distribuir nuevas claves se vuelve un problema de seguridad

Si se emplea dos veces la misma clave, un atacante puede tomar estos dos textos cifrados, ejecutar operaciones XOR entre los textos cifrados puede poner en evidencia patrones acerca de la clave y potencialmente se descifrarían los textos.

A gran escala, cuando se comparten muchos datos, la clave se vuelve inmanejable por lo extensa.