By Hendrix

Index

Bueno, me e decidido a hacer un cruso para que la gente se meta en esto de los Algoritmos y las maneras de romperlos.

Capitulo I

Dare por sabido que todo el mundo sabe que es un algoritmo, si no sabes que es habre la Wiki y busca la definición de Algoritmo.... ;) ;)

En este curso iremos subiendo de nivel, empezaremos con practicas faciles e iremos subiendo el nivel, en esta primera practica romperemos un algoritmo bastante flojo, es el metodo de encriptación que hay en la web de un amigo.

Lo que vamos a necesitar para esta practica:

- Calculadora: puede ser la del Win o alguna que tengais a mano.

- Tabla ascii: En internet hay muchisimas, para esta pracica e usado esta: http://ascii.cl/es/

Y ya esta, con esto podremos craquear facilmente ese Algoritmo.

La principal debilidad de los algoritmos on-line es que peudes introducir los datos que quieras y hacer comparaciones de los resutlados obtenidos. Evidentemente si un Algoritmo es bueno por muchas comparaciones que hagas no lo vas a sacar, por ejemplo los hashes del MD5.

Bueno, vayamos a lo nuestro...

El algoritmo a romper esta en esta pagina: http://egroj.5u.com/

Ahora empezaremos nuestro exaustivo analisis.

Se tiene que introducir una clave y el texto a encritpar, vayamos a probar uno de los Algoritmos mas comunes en los Algoritmos caseros, que son las operaciones con los caracteres ASCII.

En la clave ponemos el numero 1 y en el texto ponemos tambien el nº 1.

Damos a encritpar y nos sale 098. Bien, ahora sabemos que posiblemente este algoritmo, para desencritpar, vaya cogiendo bloques de 3 en 3 y los desencripta.

Ahora vayamos a aprofundir mas, nos vamos a la tabla ASCII y buscamos el ASCII del nº 1, que es 49, curioso, emos introducido en la clave el nº 1 (ASCII = 49) y el texto tambien el nº 1 (ASCII = 49). Si los sumamos nos da 98, que es lo que nos a salido en la Clave!! (como todos saben, un 0 a la derecha no significa nada). Vamos a provar otras cosas.

En la clave introducimos otra vez el nº 1 y en el texto a encriptar ponemos la letra a (minuscula).

Como resultado nos da 146, nos vamos a la tabla y nos da esto:

1 = 49
a = 97

Nos vamos a la calculadora, lo sumamos y...BINGO!!, nos da 146 :D :D

Parece que ya tenemos el Algoritmo medio crackeado, ahora vamos a poner una palabra, por ejemplo esto: Hendrix, y de clave le pondremos nuestro nº 1. Lo encriptamos y nos da esto:

121150159149163154169

mmmmm, un numero muy largo, no??? no se asusten, ya que antes sacamos que esto analizaba en bloques de 3. Vamos a calcular como hicimos antes:

Ascii de la letra H (mayuscula) + Ascii del nº 1 = 121
Ascii de la letra e + Ascii del nº 1 = 150
Ascii de la letra n + Ascii del nº 1 = 159
Ascii de la letra d + Ascii del nº 1 = 149
Ascii de la letra r + Ascii del nº 1 = 163
Ascii de la letra i + Ascii del nº 1 = 154
Ascii de la letra x + Ascii del nº 1 = 169

Como veis, todo estos numeros, peustos de una tacada dan el mismo numero que nos habia dado el encritpador.

Bien!! ya casi tenemos el algoritmo roto, ahora vamos a ver que pasa con una pass de mas de un numero.

En la pass ponemos esto: 12
y en el texto a encriptar esto: a

Nos da esto: 196

Evidentemente ahora solo tenemos un bloque de tres, vamos a operar en ascii

1 = 49
2 = 50
a = 97

Que operacion con estos 3 numeros nos da 196??? Facil, no?? la SUMA. Lo sumamos todo y nos da 196.

Ahora si, ya tenemos el algoritmo roto. Y para desencritparlo es lo mismo,

como sabemos que lo desencritpa en bloques de 3 vamos a intentar sacar lo que nos daria si en la Pass hubieramos peusto esto: Hen y el resutlado fuese esto: 387394391380.

H = 72
e = 101
n = 110

Ahora cojemos lso bloques de 3 en 3, y como sabemos que para encritpar los numeros se suman, ahora lo tendremos que restar (Doy por sabido que todos saben hacer equaciones de primer grado...).

72 + 101 + 110 = 283

(Este paso lo hacemos porque antes sacamos que los resutlados de la pass se sumaban).

387 - 283 = 104
394 - 283 = 111
391 - 283 = 108
380 - 283 = 97

104 es el ASCII del caracter: h
111 es el ASCII del caracter: o
108 es el ASCII del caracter: l
97 es el ASCII del caracter: a

Nuestra palabra encritpada es hola. :D :D

Ahora ya tenemos el Algoritmo roto al 100%, si quieren, se pueden hacer alguna aplicacion en algun lengauje de programación que aga esto, yo me lo hice en VB y en Perl.

Bueno, y esto es todo, hasta aqui el primer Capitulo, con un algoritmo facilito.

En los próximos capitulos posiblemente aga yo mismo los Algoritmos en archivos .exe....Si alguien tiene algun algoritmo casero que sea interesante para crakear que lo pase, evidentemente si esta bien echo posiblemente no lo logre crakear.

Otra cosa, en mis ratos libres codeo herramientas que analizar strings encritapdas y lascomparan, sacan los máximos datos posibles. Cuando pueda las posteare, ya que ayudan bastante.

Saludos y espero que les haya gustado.

Fecha de edición: 07/12/2006

Hendrix

Capitulo II

Bueno, aqui les traigo la siguiente edicion de este Cruso.

El algoritmo tampoco es gran cosa, lo e echo yo, para empezar, ya que si pongo algo dificilito alguno se va a perder, y este no es el objetivo.

el Programa lo e echo con el VB, asi que tendran que ejecutarlo forzosamente desde Windwos, si alguien usa linux que lo digo y lo hare en Perl, no lo e echo desde el principio ya que mucha gente no tiene el interprete del Perl.

Lo que vamos a necesitar para esta practica:

Usaremos lo mismo que en el capitulo I, usaremos esto en todos los Capitulos creo.

Bueno, aqui les dejo la descarga del Archivo: Descarga

Dentro del Zip les e codeado una pequeña aplicacion que nos traduce la palabra que querramos a ASCII, separando los ASCII's de cada letra por un espacio.

Lo e tenido que subir en mi segundo FTP ya que el principal esta OFF ahora. Si falla este FTP pruebenlo pasados unos minutos. ;) ;)

Una vez descargado iniciemos nuestra auditoria...

Empezaremos ponendo esta frase: Hola

Y el programa nos devuelve esto: Fqjc

Vamos a traducirlo a ASCII.

Hola = 72 111 108 97

Fqjc = 70 113 106 99

Como ven, la diferencia entre numeros es de 2, pero en unos es sumandole 2 y en otros es restandole....casualidad???camos a ver, probamos otra palabra, ahora pondremos esto: Hendrix Y nos da esto: Fglfpkv, ahora le pasamos mi aplicacion y nos da esto:

Hendrix = 72 101 110 100 114 105 120

Fglfpkv = 70 103 108 102 112 107 118

Bien, tenemos el mismo problema...Vamos a identificar las posiciones donde se

suman y las posiciones donde se restan.

En el primer ejemplo: => Suman: 2,4 Restan: 1,3

En el segundo ejemplo: => Suman: 2,4,6 Restan: 1,3,5,7

Supongo que todo ve que se agregan 2 en los numeros pares y se restan 2 en los impares....

Pues ya tenemos el Algoritmo Crakeado!!! ;D ;D

Con esta herramienta que les e codeado les hagilizara bastante la traduccion de Decimal a ASCII.... :D :D

Para el proximo capitulo se augmentara un poquito más el nivel, ya que este segundo capitulo todavia era muy básico.

Espero que les guste.

Saludos

Fecha de Edición: 07/12/2006

Hendrix

Capitulo III

Bien, aqui les traigo este neuvo tutorial. Antes de empezar les dire un par de cosas. Estos cursos sirven mas que nada para "entrenar" la intuicion a la hora de crakear un algoritmo, es evidente que kon solo mis practicas no se va a llegar a ningun sitio, las pongo para que veais como lo crakeo yo.

En este capitulo les dire como crakee el metodo de encritpación de los puertos del Poison Ivy cuando los guarda en el server.

Lo que vamos a necesitar para esta practica:

Aqui no utilizaremos la tabla ascii ya que no encripta palabras ni signos, solo numeros. Les voy a dejar una herramienta que codee para hacer un programa el cual revelase la configuracion que tenia el server del PoisonIvy 2.0.

Esta herramienta detecta los cambios que hay en 2 archivos, esto es util para localizar en donde cambian los datos, por ejemplo, si tenemos 2 servers iguales, excepto que en uno, en la pass le hemos puesto de pass: Hendrix y en el otro Gendrix, peus nos dara la posicion en el archivo donde hay ese fallo, ene ste caso nos daria donde empieza la pass del poison, ya que el poison no lo almacena al final del archivo.

Bueno, les dejo la herramienta: Descargar

Lo e tenido que subir al host viejo ya uqe con el nuevo e tenido problemas, haber si lo soluciono pronto, si no les sale la descarga pruebenlo pasados unos minutos.

Ahora les explicare lo que hice.

Lo que hice fue poner el puerto 1000 en uno y el puerto 2000 en el otro, y todos los otros campos iguales en ambos servidores.

Le pase mi herramienta y vi que cambiaba en 2 posiciones, lo habri con un editor hexa en las direcciones que me habia dado mi herramienta y vi que me daba 2 resultados en hexa, que pasados a Decimal (no se en otros editores, pero en el Hex Workshop si se tiene que pasar ya que los resultados de la izquierda estan en valor hexadecimal del resutado de la derecha que es el real). Lo pase a decimal a los 2 numeros, hice un par de pruebas mas y recolecte esta información:

232 3 = 1000
208 7 = 2000
184 11 = 3000
172 13 = 3500
160 15 = 4000
148 17 = 4500

136 19 = 5000
124 21 = 5500
112 23 = 6000
100 25 = 6500
88 27 = 7000
76 29 = 7500
64 31 = 8000
52 33 = 8500
40 35 = 9000
28 37 = 9500

Hay relacion en cada linea, por ejemplo, de 1000 a 2000, a 3000, a 4000....consiste en restarle 24, y en el de la izquierda sumarle 4, esta relación fue la culpable de que perdiera 15 minutos...xD xD xD

Luego dije, vamos a poner puertos de uno en uno, que creo que ya se como va. Saque mas puertos y obtuve esto:

179 21 = 5555
180 21 = 5556
181 21 = 5557
182 21 = 5558
183 21 = 5559
184 21 = 5560
185 21 = 5561
186 21 = 5562
187 21 = 5563
188 21 = 5564
189 21 = 5565
199 21 = 5575
202 21 = 5585
255 21 = 5631
00 22 = 5632

Si os fijais, despeus del 255 de la derecha pasa al 00 y se le suma uno al de la derecha, efectivamente pasaba lo que yo me imagine, el 255 corresponde al numero FF en hexa, despues del FF se pasa al numero 100, pues en lugar de poner 100 se ponen 00 y se le suma uno al de la derecha.

Ahora, ya podemos sacar una formula matematica, aqui se la dejo:

((255*Y)+Y)+X = Puerto

Donde Y es el numero de la derecha y X es el numero de la izquierda, al aplicar eso nos da el puerto insertado.

Y ya esta, esta es la formula que utiliza el Poison para no tener que ocupar tanto espacio en el servidor, con 2 numeros (utiliza el codigo ascii, asi que solo

ocupa una posicion por cada numero de columna, sea 1 o sea 255).

Seria interesante que los que sepan programar ideasen un algoritmo para a partir de un nuermos obtener otros 2 que mediante este algoritmo que e explicado los encripte. Asi aprenderan a aplicar la programación a la criptografia.

Bueno, esto es todo por hoy, e tardado unos cuantos disa en sacar este capitulo porque e estado algo ocupado. Espero que practiquen, ya que como dije esto no enseña a crakear, esto ams bien enseña a pensar como crakear mediante ejemplos.

Saludos

Fecha de Edición: 18/12/2006

Hendrix

Capitulo IV

Bien, aqui llega mi cuarto tema. En este romperemos un algoritmo que cree yo mismo, lo que teien en marticular es que puede tener mas de una clave encritpada por cadena a encritpar y no crashea, despues veran porque...

Lo que vamos a necesitar para esta practica:

- Tabla ascii
- Claculadora de Windows

Bien, la aplicacion que "romperemos" la la tienen que descargar de aqui.

Los botones que utilizaremos seran solo los de Encriptar texto y Desencritpar texto, los otros sirven para encritpar y desencritpar archivos con esta herramienta.

Bueno, vamos a empezar nuestro analisis, empezaremos con una cadena normal, la que queramos, para ver como funciona, yo empezare con la cadena Hendrix.

Leyenda:

CO = Clave original
CE = Clave encriptada
CD: Clave en Decimal
CH: Clave en Hexa

CO: Hendrix
CE: 01503302F03602E04004701D04F023017052076002

Bien, como vemos, es demasiado larga como para empezar nuestro analisis, y es muy probable que tengamos que hacer varios analisis (lo ultimo que crakee tuve que hacer 30 comparaciones para sacar el algoritmo).

Vamos a provar con algo mas corto:

CO: a
CE: 01C045

Aqui vemos algo bastante interesante, un 0 a la izquierda, como todos saben no tiene funcion un 0 a la izquierda, pero en algunos casos si, por ejemplo, en encriptacion por bloques.

Vamos a sacar el Ascii de la letra a: 97

Lo pasamos a Decimal a la cadena obtenida y vemos esto:

114757

Esto no tiene mucha relacion.

Vamos a probar con otra frase:

CO: z
CE: 038042

La teoria de que el 0 es una marca de encriptacion por bloques empieza a tomar fuerza, ya que si los dividieramos por 3 nos daria esto:

038 y 042, curioso que los 2 empiecen por 0, no???

Como no somos conformistas vamos a analizar algo mas:

CO: az
CE: 01C045038042

Ahora parece casi definitiva, si lo dividimos en bloques de 3 nos da esto:

01C, 045, 038 y 042.

Bien, nos fiaremos de eso y lo pasaremos a decimal.

CH: 01C, 045, 038 y 042.
CD: 28 69 56 66

Bien, ahora vamos a ver como mezclamos esto para que nos de az.

Si pasamos az a Ascii obtenemos esto:

  97 122
01C, 045, 038 y 042.
28 69 56 66

Si eliminamos la fila de los hexa casi ya tenemos el algoritmo, fijaros:

  97 122
28 69 56 66

Casualmente si le metemos el simbolo + entre cada par de bloques decimales nos da el numero de arriba, miren:

28+69 = 97

56+ 66 = 122

Aqui tenemos el algoritmo!!!! si quieren, prueben con otras frases haber si les funciona. Recuerden los pasos:

1º Pasamos los **bloques de 3** de Hexa a Decimal
2º Pasamos las letras insertadas a ascii
3º Sumamos los pares de Decimal para que nos de el nº ascii.

Bueno, y esto es todo, es algo corto porque a este algoritmo lo habia echo yo y e ido bastante "directo".

Saludos

Fecha de Edición: 23/12/2006

Hendrix

Capitulo V

Bueno, llegamos al capitulo V.

En este capitulo vamos a analizar un algortmo de un amigo que me lo paso por MP.

Lo que vamos a necesitar para esta practica:

Necesitaremos el programa de mi amigo: Descargar

Tambien necesitaremos el Notepad y el programa de la segunda practica que te pasaba los caracteres a ascii.

Bien, abrimos el programa, y escribimos esto:

A

y nos devuelve:

T

Ahora nos vamos a mi herramienta y nos encontramos esto:

A: 65
T: 84

La resta de estos 2 es: 19

Vamos a analizar mas:

B y nos da W

B: 66
W: 87

Si lo restamos: 21

Vemos que e no es igual, que es 21. Analizamos otra mas:

C y nos da Z

C: 67
Z: 90

La resta es 23

Que tienen en comun 19, 21 y 23?? Que se le suman 2, bien, ahora como escribimos el algoritmo???Con los datos que tenemos aun no podemos hacer nada, vamos a analizar una cadena, lo que voy a utilizar yo es todo el Abecedario en mayusculas, y nos dara esto:

65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90

Y los asciis de la cadena encriptada:

84 87 90 93 96 99 102 105 108 111 114 117 120 123 126 129 132 135 138 141 144 147 150 153 156 159

Bien, para llegar a la conclusion siguiente tuve que pensar bastante, si se fijan el nº 1 en la ultima posicion (por ejemplo el nº 71 lo tiene) representa el nº 2 al final del numero en la cadena encriptada (por ejemplo 102). Pues bien, si pasamos de 71 a 81, usamos 10 numeros, pero si hacemos lo mismo en la cadena encriptada nos dara que pasamos 30, (de 102 a 132).

Pues bien, ahora si nos vamos al primer numero de la cadena encriptada tendremos es 60% del algoritmo, como lo hacemos??? si sabemos que por cada x numeros desplazados en la cadena encriptada son X/3 en la cadena normal vamos a hacer esto:

estamos en 102, queremos pasar a 0, lo que aremos sera lo siguiente:

102/3 = 34

Y ahora, el 102 representa al 71, pues si le restamos 34 al 71 nos da 37.

Es decir, que el nº 0 en la cadena encriptada es el ascii 37, nos vamos al prgorama, en la linea de introducir codigo y pulsamos Alt + 37, soltamos el alt y se escribe un caracter (este %), si estamos en lo correcto, al pulsar en encritpar no saldra nada en el resultado (esto corresponde al ascii 0)., lo pulsamos y efectivamente no nos aparece nada.

Ahora probamos, ponemos el ascii 38 (&), le damos a encritpar y el ascii del simbolo que nos sale es 3, ahora probamos con el ascii 39 ('), lo encritpamos y nos da 6, y ya esta, ya tenemos el algoritmo!!! El algoritmo es:

(x-37) * 3

Probemoslo:

Ascii 65

(65-37) * 3

Nos da 84!!!

Ascii 66

(66-37) * 3

Nos da 87!!!!

Ya esta, ya emos crakeado este algoritmo.

Saludos

Fecha de Edición: 27/12/2006

Hendrix

Despedida

Bueno, ya se a terminado este "mini-curso" de introduccion al analisis de los algoritmos de encriptacion, quiero decir que hay infinitos algoritmos (y maneras de programarlos), asi que posiblemente casi nunca se encuentren algoritmos de los tipor que e explicado aquí, con este curso (y vuelvo a reiterar) es solo para "abrir" sus cabezas, para que piensen a la hora de analizar un algoritmo, ahora solo ustedes ponen el limite de difucultad.

Saludos a todos.