EXAMEN PARCIAL SEGURIDAD EN COMPUTACIÓN

CICLO 2017-1

ALUMNO: Felipe Moreno _____ CÓDIGO: 20120354I_____	Nota: 20

Pregunta 1.-

Dadas las siguientes ACL's y C'list, arme la correspondiente Access Control Matrix

Recurso	Read	Write	Execution
Cache	Arturo Maritza		Maritza
Heap	Norma		Peter
File: Segments	Arturo Maritza		Arturo
File: \syscpk	Peter	Maritza Julio Norma Peter	Julio
File:\Message	Norma	Norma	Norma

Ente	Read	Write	Exec
Arturo	Cache File:Segments		File:Segments
Maritza	Cache File: Segments	File:\syscpk	Cache
Norma	Heap File:\Message	File:\syscpk File:\Message	File:\Message
Peter	File:\syscpk	File:\syscpk	Heap
Julio		File:\syscpk	File:\syscpk

Sol:

Ente	Cache	Heap	File: Segments	File: \syscpk	file: \Message
Arturo	R--	---	R-X	---	---
Maritza	R-X	---	R--	-W-	----
Norma	---	R--	---	-W-	RWX
Peter	---	--X	---	RW-	---
Julio	---	---	---	-WX	---

Pregunta 2.-

Algoritmo hashcash

Hashcash es un sistema de proof-of-work inicialmente diseñado en 1997 para limitar el spam en el correo electrónico o los ataques de denegación de servicio. Se trata de un método mediante el cual se añade información extra al encabezado de un correo electrónico para probar que el emisor legítimo ha invertido una cierta capacidad de cálculo para enviar el mensaje. Si se demuestra este hecho, implica que el emisor no es un spammer.

Tomando un algoritmo de hash, hashcash exige que el emisor calcule un hash que contenga 20 bits a cero a la izquierda. La única forma que tiene el emisor de generar esta información es a través de aplicar iterativamente el algoritmo de hash (fuerza bruta) sobre la información original e incrementar iterativamente un entero hasta que el resultado del cálculo (el hash) cumpla la condición del número de bits a cero anterior. El receptor puede verificar que esta información es efectivamente válida con un coste computacional insignificante, equivalente a un único hash. En cambio, el emisor tiene que realizar 220 hashes en media hasta encontrar un resultado válido. Ya que el tiempo de generación de un único hash es predecible (dependiendo de la capacidad de cálculo disponible), el tiempo necesario para generar el hash con 20 ceros a la izquierda es predecible en media. De esta manera, si el emisor se ha tomado la molestia de generar esta información con la carga de trabajo que conlleva, se demuestra que no es un spammer. En cambio, para un spammer, la capacidad computacional necesaria es lineal con respecto al número de emails a enviar, lo que implica que el trabajo se ralentiza y el uso de recursos aumenta considerablemente, haciendo que la viabilidad de enviar correo no deseado no sea realmente tan positiva en la práctica. Por ejemplo:

"Hello, world!0" =>
1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64

"Hello, world!1" =>
e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8

"Hello, world!2" =>
ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7

...

"Hello, world!4248" =>
6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965

"Hello, world!4249" =>
c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6

"Hello, world!4250" =>
000003af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9

En el ejemplo práctico anterior, se puede observar como el emisor tendría que cambiar el Nonce hasta 4251 veces y generar la misma cantidad de hashes hasta encontrar un resultado con el número de ceros a la izquierda especificado.

Utilizando su algoritmo de MD5, realice una implementación de HashCash, añadiendo un entero al final de su nombre y código de alumno en mayúsculas, hasta obtener un hash cuyo primer byte sea cero.

Input: **FELIPE MORENO 20120354I**

Número de intentos:**150**

MD5: **00e6e74268ec5e93e13c35f187cda897**

Pregunta 3.-

Haga un programa que genere un cifrado RC4 haciendo XOR con cada uno de los bytes provistos por el algoritmo. Deseche los primeros 1024 bytes del generador.

Encriptar el siguiente mensaje:

> “LOS MOLINOS DE VIENTO EN TU MENTE”

Realizar la encriptación usando la siguiente clave: ELECCIONES

Respuesta: (En Hexadecimal):

4C8E60896984C702C17D654503ABF578E06A3FE7A02141E66FA8CF5B8BEDCFB8A06

Pregunta 4.-

Utilizando El Gamal envíe un mensaje al profesor. Utilice las claves publicadas en el gnomio. Copie los datos en un archivo de texto (todo le necesario para evaluar si estuvo bien)

Mensaje original:

Hola mi nombre es juan cachaporras y se que por ahi me andan diciendo que yo soy la muerte la destructora de mundos portadora de desastres y del caos inminente ... Ademas de eso, me llaman el demonio de la ciudad gris, sediento y hambriento

Mensaje encriptado:

4fb76ac023046d052e647147ef81cdb1ea7da07c903173b48b26a8719481030803187594b5382aefcc7186ca9c75a955e5023888faff94fe38af2a46af7765d6b4100afa7804ea1c616bd51624a57f3de9ac07c23f589117916f74c83826f49de90ed3cb82095a23ff8e4d051c20b1b0b55264babaee55a976838f435f9c0f0f7b44a928230f3d0e7c985bf97e476280422bcab552e50e5e2d1b667a4a6563e0c0f417c6bf5ce1575f7c12e9560d299b73a24e0d85949d2bf28669fcfe084eda6df67229214bc2518fc10ceed85e27adf936a45eddbeccc7162abf875dc525b8f1fb3c3a2c8f7cf02592459b60fb153

Ys: clave de sesion:

278621e9f8426240555f9279642ae77d579d50ebe68a6dc00f63da7c05e026e146af38b2c85dcba48278a17

Metodo de encriptación: RC4 (normal)

Generador: **7**

Primo: **oakle 2**

ffffffffffffffffc90fdaa22168c234c4c6628b80dc1cd129024e088a67cc74020bbea63b139b22514a08798e3404ddef9519b3cd3a431b302b0a6df25f14374fe1356d6d51c245e485b576625e7ec6f44c42e9a637ed6b0bff5cb6f406b7edee386bfb5a899fa5ae9f24117c4b1fe649286651ece65381ffffffffffffffff

clave pública: Ya

76865e2b27136f8a82ab218a184439518a603cdea195b9015a74f1d134cf861085f85c1cafb94efbb772f9d6e14ccad52f9f72f3692ac20ceade857895ef622e802e0e18655d5c4253cc6c9b6ed3d86f6e45d76bab9dd624f18afda52190aa46ce298f22837d22e086211925592c4ef9619c74b9b33589a1789f1f3b752a2aea

Pasos de encriptacion, una vez generado el S, el Ys con su clave publica en el fichero ClavesPublicas, encrypte usando RC4(S,mensaje) y ese mensaje cifrado lo transforme a hexadecimal tomando uno por uno cada carácter del mensaje cifrado.

(adjunto una carpeta con mi codigo, para que haga pruebas)

Pregunta 5.-

Implemente un programa para introducir un mensaje y una clave. El programa generará un HMAC de 16 bytes usando el RFC-2104.

El mensaje es: “FINAL DE LA CHAMPIONS LEAGUE”, utilice como clave su código de alumno en MAYÚSCULAS.