



Universidad Nacional Autónoma de México

Facultad de Ingeniería

Materia: Sistemas Operativos

Nombre del Profesor: ING. Gunnar Eyal Wolf

Iszaevich

Semestre 2022-2

Exposición: Quantum Key Distribution

Fecha de entrega: 12/05/2022

Nombre del alumno:

Ø Alemán Flores Carlos Eduardo

Ø Pérez Duarte Brenda Elizabeth

Introducción:

Orígenes de la criptografía

Si bien no se sabe quiénes fueron los primeros en comunicarse de manera secreta, se sabe que los espartanos fueron pioneros en la criptografía en Europa, creando un dispositivo llamado escítala, este consistía en un bastón en el que se enrollaba una tira de papel o cuero que contenía un mensaje, la tira mostraba un mensaje revuelto, pero al enrollarlo en el bastón éste mostraba el mensaje.

Otro método de cifrado fue el llamado Cifrado César, el cuál consistía en reemplazar una letra por otra, desplazando un cierto número de letras, por ejemplo, reemplazar la A con la D y la B con la E al desplazar 3 letras.

Estos métodos son ahora llamados transposición (escítala) y sustitución (cifrado César), la sustitución simple es fácil de descifrar puesto que sólo existen 26 combinaciones, otro método de descifrar los cifrados monoalfabéticos fue propuesto por Al-Kindi, quien notó que al sustituir una letra por otra, ésta mantenía sus características, por lo que por un análisis de frecuencia en las letras se podía determinar la sustitución, por ejemplo, en inglés la letra más común es la E con una frecuencia de 12.7%, por lo que si alguna letra tiene una frecuencia similar en el mensaje, probablemente se trate de la E.

Tiempo después nacerían los cifrados polialfabéticos, en los que cada letra tiene una sustitución diferente, por ejemplo, la primer letra se desplaza 4 lugares, la segunda 9 y la tercera solo 1, y así se repite durante todo el mensaje; 4, 9 y 1 sería considerada la llave criptográfica, este método puede hacer que 2 letras diferentes sean sustituidas por la misma letra, por lo que el análisis de frecuencia ya no sería útil. Durante muchos años fue considerado como "El cifrado indescifrable".

Para romper el cifrado polialfabético se tiene que determinar el tamaño de la llave criptográfica, para esto podemos cifrar alguna cadena, por ejemplo, TOBEORNOTTOBE, al cifrar podemos obtener ACULCVUCMACUL, observamos que la secuencia ACUL se repite en una distancia de 9, por lo que el tamaño de la llave debe ser de 9, 3 o 1, se aplica un análisis de frecuencia a cada tercer o noveno carácter y alguno revelará el mensaje, esto se complica cuando se tienen llaves de tamaño mucho mayor.

Sin embargo sí existe una manera de hacer cifrados indescifrables, estos son hechos con un "one-time pad", éstos están basados en el alfabeto binario, el mensaje es convertido en unos y ceros y se crea una llave de unos y ceros de la misma longitud que el mensaje, para cifrar se suma el mensaje con la llave basados en las reglas de suma de números binarios, para descifrar el mensaje se suma el mensaje cifrado con la llave y así obtenemos el mensaje original, Claude

Shannon, quien descubrió que existían los cifrados indescifrables, estipuló que si la llave es secreta, de la misma longitud que el mensaje, aleatoria y no se vuelve a usar, entonces el one-time pad es indescifrable.

El problema con éste método es el "Problema de distribución de llave", ya que los usuarios tienen que acordar previamente una llave para poder realizar el cifrado y transmitir el mensaje con seguridad, pero el acuerdo entre usuarios para la llave resulta problemático, ya que incluso si se tiene una línea segura nunca se sabe si realmente es segura, ya que ésta puede ser monitoreada de forma pasiva y ni el remitente ni el receptor podrían notar que hay alguien escuchando, esto debido a las propiedades de la física clásica, las cuales dictan que al medir un objeto no alteramos sus propiedades.

Un método usado para evitar el problema de la distribución de llave es el protocolo RSA, el cual nos da una llave pública, para cifrar el mensaje y una llave privada para descifrarlo, el problema con este protocolo es que basa su seguridad en la dificultad de las computadoras en factorizar números grandes, por lo que si se propone un método más rápido para factorizar, la seguridad dejaría de existir, por lo que la confianza en RSA se sostiene en la lentitud en el progreso tecnológico, ya que en cuanto se comiencen a usar computadoras cuánticas se podrá romper el RSA.

Distribución cuántica de llave (Quantum Key Distribution)

Los principios de la física cuántica nos dicen que la observación de un estado cuántico causa perturbación de este. Por lo que varios protocolos de QKD están diseñados para asegurar que los intentos de un espía al observar los fotones transmitidos causen perturbación en la transmisión, para que los usuarios legítimos puedan detectarlo. Para hacer de QKD aún más segura, se puede combinar con el One Time Pad, sin embargo, esto puede causar limitaciones con el ancho de banda, ya que el OTP debe ser tan largo como el mensaje y la distribución de QKD es entre mil y diez mil veces más lenta que otras comunicaciones.

La QKD ha sido comercializada por empresas como IDQ desde el 2007, usada para asegurar las elecciones en Ginebra del 2007 y ha sido usada desde entonces, otros usuarios de la QKD son bancos y gobiernos alrededor del mundo.

Máquina Cuántica

Uno de los principales motivos para la construcción de una computadora cuántica es que la máquina cuántica usa superposición [permite que los algoritmos cuánticos utilicen otros fenómenos de la mecánica cuántica, como la

interferencia y el entrelazamiento (Los qubits entrelazados siempre se correlacionan entre sí para formar un único sistema. Incluso cuando están infinitamente alejados uno de otro, la medición del estado de uno de los cúbits nos permite conocer el estado del otro, sin necesidad de medirlo directamente.)) que crean una capacidad de cálculo que puede solucionar problemas con una velocidad exponencialmente más rápida que la de los equipos clásicos, y posibilidades enredadas que pueden agilizar tremendamente la factorización de 2 números primos muy largos. Para darnos una idea un típico número de 640 bits compuesto por 2 número primos necesita de aproximadamente 2.2 GHz opteron CPU (microprocesador x86 en ADM) que se traduce a 5 meses.

El fácil proceso de multiplicar 2 números primos largos es usado para encriptar información secreta o segura, por ejemplo, la tarjeta de crédito.

Para decodificar la información se necesita el proceso inverso de la factorización y esto es difícil. En este caso, la información es segura siempre y cuando el esquema de encriptación cambie regularmente.

Qubit

Un qubit puede verse como una partícula cuántica que no está limitada por 2 estados, pero en principio puede tener cualquier número de niveles discretos. Los fotones son excelentes para la comunicación cuántica como transmitir sobre distancias largas con pocas perdidas y sin ningún mecanismo de incoherencia conocido en el espacio libre.

Una ventaja de los qubits es la gran cantidad de información que contiene y que solo un portador cuántico puede transmitir. Un simple sistema cuántico, como el fotón, tiene el potencial de cifrar una cantidad arbitraria de información.

La teletransportación cuántica fue propuesta en 1993 por Bennett y es un importante protocolo con aplicaciones en redes cuánticas y computación cuántica. Permite a Alice y Bob (si comparten un estado enredados) a distribuir arbitrariamente un estado cuántico sin mandarlo, solo mandando información clásica.

La no demolición cuántica (QND) es otro protocolo de transportación donde el estado cuántico no es destruido y la información cuántica restante, que está almacenada en otros niveles, está intacta y puede transmitirse en los siguientes pasos.

Esquemas de Encriptación:

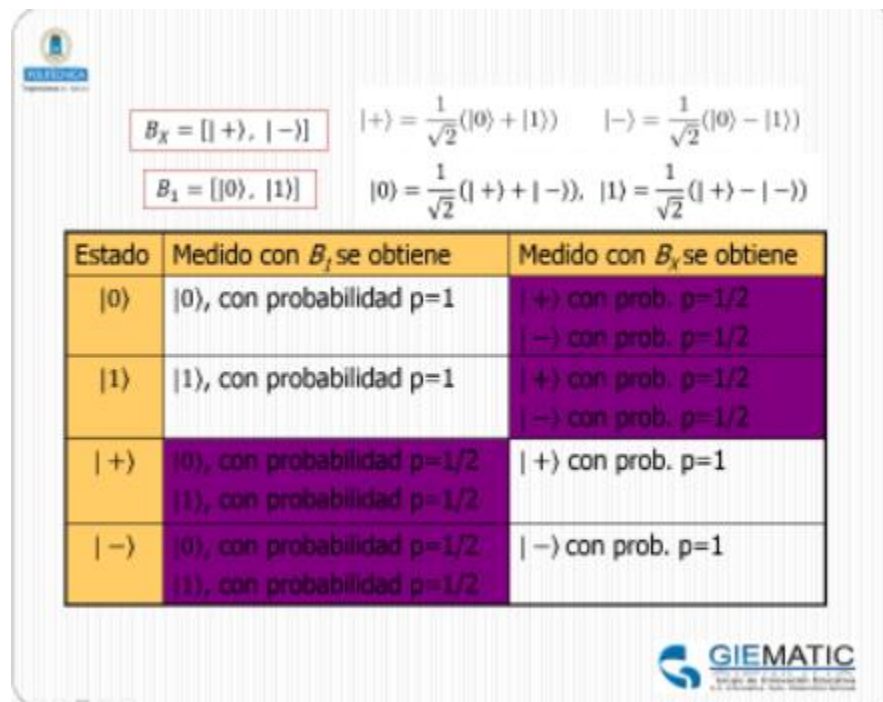
2 esquemas básicos de encriptación son el esquema Bennett - Brassard en 1984 (BB84) o el esquema de Ekert.

Esquema Ekert:

Existe la desigualdad de Bell, que en el protocolo de Ekert, esta desigualdad es usada para checar que un estado entrelazado cuántico compartido entre 2 partes no se viole y esto es importante porque se sabe que un one time pad consiste en una serie de números aleatorios compartidos entre 2 partes que sirven como una llave de seguridad para cifrar o descifrar mensajes.

Protocolo BB84

En el espacio de Hilbert H_1 (generalización del concepto de espacio euclidiano) consideramos las dos bases ortogonales más usuales: la base $B_1 = [|0\rangle, |1\rangle]$ ket 0 o 1, que se identifica con la polarización horizontal y vertical, y la base $B_x = [|+\rangle, |-\rangle]$ ket + o - identificada con la polarización 45° y -45°



$B_x = \{|+\rangle, |-\rangle\}$
 $B_1 = \{|0\rangle, |1\rangle\}$

$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
 $|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$

$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
 $|1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle)$

Estado	Medido con B_1 se obtiene	Medido con B_x se obtiene
$ 0\rangle$	$ 0\rangle$, con probabilidad $p=1$	$ +\rangle$ con prob. $p=1/2$ $ -\rangle$ con prob. $p=1/2$
$ 1\rangle$	$ 1\rangle$, con probabilidad $p=1$	$ +\rangle$ con prob. $p=1/2$ $ -\rangle$ con prob. $p=1/2$
$ +\rangle$	$ 0\rangle$, con probabilidad $p=1/2$ $ 1\rangle$, con probabilidad $p=1/2$	$ +\rangle$ con prob. $p=1$
$ -\rangle$	$ 0\rangle$, con probabilidad $p=1/2$ $ 1\rangle$, con probabilidad $p=1/2$	$ -\rangle$ con prob. $p=1$

El protocolo BB84 se puede describir del siguiente modo:

Paso 1: Alicia genera una cadena aleatoria de ceros y unos (por ejemplo lanzando una moneda al aire).

Paso 2: Para cada bit de la cadena, Alicia elige aleatoriamente una de las dos bases B_1 o B_x y envía a Bob, por un canal cuántico, el qubit correspondiente, mediante un fotón polarizado, de acuerdo con el siguiente alfabeto:

- Si ha elegido B_1 : el 0 lo codifica como $|0\rangle$ (polarización horizontal) y el 1 como $|1\rangle$ (polarización vertical).
- Si ha elegido B_x : el 0 lo codifica como $|+\rangle$ (polarización 45°) y el 1 como $|-\rangle$ (polarización -45°).

Cuando Bob recibe cada fotón, no tiene modo de saber con qué alfabeto ha sido codificado, así que él lo mide eligiendo, también aleatoriamente, para cada uno de ellos la base B_1 o B_x . Aproximadamente la mitad de las veces Bob elegirá la misma base que Alicia y la otra mitad elegirá la base contraria a la utilizada por ella.

Paso 3: Para localizar y eliminar los bits en que las mediciones se han realizado con distintas bases, se realiza el proceso de contraste de información, denominado sifting o Reconciliación de bases.











Bob comunica a Alicia, por el canal clásico, qué base ha usado en cada medición.

Como respuesta, Alicia le comunica las posiciones en las que ella ha usado la misma base. En estas posiciones, Alicia y Bob deben tener bits coincidentes.



Paso 4: Alicia y Bob borran de sus cadenas los bits en los que se han usado bases diferentes y se quedan con el resto. De este modo, si no ha habido ruidos ni interferencia de espías, tienen una clave común, que denominamos clave bruta, cuya longitud será aproximadamente la mitad de la de la cadena inicial.

Un ejemplo

Mensaje	0	0	1	0	1	1	0	0	0	1
Base elegida	B_1	B_X	B_1	B_X	B_1	B_X	B_1	B_1	B_X	B_X
Codificación	$ 0\rangle$	$ +\rangle$	$ 1\rangle$	$ +\rangle$	$ 1\rangle$	$ -\rangle$	$ 0\rangle$	$ 0\rangle$	$ +\rangle$	$ -\rangle$
Polarización										
B mide con	B_1	B_1	B_X	B_X	B_X	B_1	B_1	B_1	B_X	B_X
Resultado	$ 0\rangle$	$ 0\rangle$	$ +\rangle$	$ +\rangle$	$ -\rangle$	$ 0\rangle$	$ 0\rangle$	$ 0\rangle$	$ +\rangle$	$ -\rangle$
Reconciliación	0			0			0	0	0	1

Eva

Existe la posibilidad de que un espía, que convencionalmente es llamada Eva, intercepte los qubits enviados por Alice, los mida y los reenvíe a Bob, sin embargo, por propiedades de la cuántica, al medirlos Eva podría modificar el estado del qubit, teniendo los siguientes escenarios:

- Eva mide el qubit en el mismo eje que fue preparado el qubit, por lo que no perturbaría el estado inicial del qubit, regresando el qubit a Bob pasando inadvertida.
- Eva mide el qubit en el eje contrario al que fue preparado, destruyendo el estado inicial, sin saberlo, regresa el qubit a Bob, si Bob mide en un eje diferente al que fue preparado por Alice, Eva pasa desapercibida ya que se descartaría ese qubit.
- Eva mide el qubit en el eje contrario al que fue preparado, lo regresa a Bob, si Bob mide en el eje que fue preparado originalmente, puede obtener, con un 50% de probabilidad el estado original, por lo que Eva pasaría desapercibida.
- Eva mide el qubit en el eje contrario al que fue preparado, lo regresa a Bob, si Bob mide en el eje que fue preparado originalmente y no obtiene el estado en el que fue preparado por Alice, por lo que Alice podría darse cuenta y detener el protocolo.

Por lo tanto, con un qubit, Eva tiene un 25% de probabilidad de ser descubierta, pero, con 10 qubits, la probabilidad aumenta a un 95% y con 50 qubits aumenta a 99.9999% de ser descubierta.

Métodos de espionaje y su mitigación

- Clonación de qubits
 - Clonar los qubits enviados por Alice, enviar los originales a Bob y medirlos hasta que hayan publicado los resultados.
 - No se pueden clonar qubits si no se conoce su estado.
- Envío de otros qubits
 - Tomar los qubits enviados por Alice, enviar qubits diferentes a Bob y medir los qubits de Alice cuando hayan publicado los resultados.
 - Habría grandes diferencias entre los valores de Alice y Bob, lo que abortaría el protocolo.
- Medición de menos qubits
 - Medir una menor cantidad de qubits, haciéndolo de forma salteada para disminuir la probabilidad de ser descubierta.
 - Aumentar los qubits de seguridad aumentaría la probabilidad de descubrirla.
- Ataque de escisión del número de fotones
 - Al preparar los qubits puede que se programen en más fotones, ya sea para soportar la disipación del canal o porque el emisor envíe más.
 - Eva podría tomar solo uno de los fotones, dejando pasar los demás, pasando desapercibida.
 - Se realiza un conteo de los fotones enviados y recibidos.
- Ataque del caballo de Troya
 - Consiste en enviar pulsos de luz por el canal hacia el emisor con el fin de sondear como está configurado el emisor de fotones, obteniendo el eje con el que debe medir.
 - Se implementa un canal de una sola dirección.

Referencias:

- QUANTUMFRACTURE. (2019). HACKEANDO MENSAJES CUÁNTICOS: LA VENGANZA DE EVA. RETRIEVED 9 MAY 2022, FROM [HTTPS://WWW.YOUTUBE.COM/WATCH?V=IBUVXJ0VXFC&AB_CHANNEL=QUANTUMFRACTURE](https://www.youtube.com/watch?v=IBUVXJ0VXFC&AB_CHANNEL=QUANTUMFRACTURE)
- QUANTUMFRACTURE. (2019). CÓMO MANDAR UN MENSAJE SECRETO CON FÍSICA CUÁNTICA | ENCRIPCIÓN CUÁNTICA. RETRIEVED 9 MAY 2022, FROM [HTTPS://WWW.YOUTUBE.COM/WATCH?V=7R7DNT2043M&AB_CHANNEL=QUANTUMFRACTURE](https://www.youtube.com/watch?v=7R7DNT2043M&AB_CHANNEL=QUANTUMFRACTURE)

- QKD TECHNOLOGY. RETRIEVED 9 MAY 2022, FROM [HTTPS://WWW.IDQUANTIQUE.COM/QUANTUM-SAFESECURITY/QUANTUM-KEY-DISTRIBUTION/](https://www.idquantique.com/quantum-safe/security/quantum-key-distribution/)
- GARCÍA, A., GARCÍA, F., & GARCÍA, J. (2014, 24 JUNIO). MOOC CRYPT4YOU UPM. CRYPT4YOU AULA VIRTUAL. RECUPERADO 9 DE MAYO DE 2022, DE [HTTP://WWW.CRIPTORED.UPM.ES/CRYPT4YOU/TEMAS/CUANTICA/LECCION2/LECCION02.HTML](http://www.criptored.upm.es/crypt4you/temas/cuantica/leccion2/leccion02.html)
- MICROSOFT. (S. F.). ¿QUÉ ES UN QUBIT? | MICROSOFT AZURE. MICROSOFT AZURE. RECUPERADO 9 DE MAYO DE 2022, DE [HTTPS://AZURE.MICROSOFT.COM/ESMX/OVERVIEW/WHAT-IS-A-QUBIT/#SUPERPOSITIONINTERFERENCE-ENTANGLEMENT](https://azure.microsoft.com/esmx/overview/what-is-a-qubit/#superpositioninterference-entanglement)
- PETRITSCH, K. (2018). QUANTUM INFORMATION SCIENCE: THE NEW FRONTIER IN QUANTUM COMPUTATION, SECURE COMMUNICATION, AND SENSING. ARCLER PRESS.
- SERGIENKO, A., V. (2005). QUANTUM COMMUNICATIONS AND CRYPTOGRAPHY. CRC PRESS.