Seguridad en Redes Inalámbricas

Bruno Medina Bolaños Cacho

9 de octubre de 2012

Índice general

Capítulo 1

Introducción

1.1. Seguridad de la Información

Cuando se habla de seguridad en cualquier ámbito, se hace referencia a un entorno libre de amenazas, peligros o daños. En la vida práctica, estos ambientes son virtualmente inexistentes, pues con probabilidad positiva (aunque pequeña) siempre existirán riesgos o imprevistos que pudieran afectarlos. Sin embargo, para usos prácticos se descartarán estos improbables eventos y se retomará el concepto general.

Tómese el ejemplo del propio hogar. De la forma más natural se asocia al hogar como ese entorno **seguro** donde se puede realizar cualquier actividad en el momento que se plazca sin ser víctima de algún daño. Lo que muchas veces se olvida, gracias al grado de confianza que se adquiere a la benevolente falta de reacción de nuestros descuidos, es que dicha seguridad proviene de la protección que se provee para el hogar.

La protección del hogar se logra a través de varios mecanismos, como: las paredes que delimitan el entorno, los múltiples seguros instalados en las chapas e incluso los complicados sistemas de alarma que estallan con el pasear de un roedor. Este tipo de mecanismos garantizan esa seguridad y permiten a los residentes realizar sus actividades cotidianas sin temor a sufrir incidentes desagradables.

De la misma manera, así como se busca la seguridad de nuestros seres queridos. Se ha buscado desde hace siglos, proteger información sensible. Y es que desde que la información ha tenido valor, los humanos han tratado de ocultarla, ya fuera para mantener secretos, para establecer comunicación entre los individuos de sus grupos, e incluso para garantizar su acceso personal.

La criptografía ha estado con nosotros desde hace miles de años. Gracias a ella se han escondido: fórmulas secretas, opiniones religiosas, mensajes de guerra, y hasta cartas de amor. Hoy en día a cada instante y sin darnos cuenta, la usamos en la mayoría de nuestros dispositivos electrónicos. Por ejemplo: Las llamadas de celular, son cifradas y enviadas a través del aire. Los vehículos automotores no encienden sin los mecanismos

que se encuentran en sus llaves. Y ni empecemos con los mecanismos de seguridad que se utilizan para resguardar nuestro dinero, ¡cómo el peso de nuestro colchón!

De la misma manera, desde que la era de la información se apropió de nuestro mundo, la seguridad de la información ha sido cada vez más importante. Hemos llegado al punto de considerar más verídico lo que sucede en nuestra realidad virtual, que lo que observamos en nuestro mundo cotidiano. La tendencia implica una necesidad por una mayor **privacidad**, un mayor control de los observadores de nuestras historias. Una mayor seguridad en los sistemas de información que nos proveen la entrada a nuestro nuevo mundo virtual.

Los sistemas de información que utilizamos son muchos, cada uno de ellos provee de alternativas y distintos mecanismos de protección, a estos mecanismos informáticos se les llama: **Criptosistemas**.

En la literatura y a través de los años, se ha llegado a la conclusión de que cualquier **criptosistema** deberá cumplir con estos cinco objetivos primordiales:

- **Confidencialidad:** Una vez que se haya cifrado el mensaje, el mensaje podrá ser leído **únicamente** por el destinatario.

- **Integridad de datos:** Todo mensaje enviado jamás podrá ser manipulado o alterado, ya sea por algún error de transmisión o por algún atacante. En general, los criptosistemas utilizan funciones que permiten detectar cualquier tipo de error o manipulación.

- **Autenticidad:** Siempre se deberá verificar la autenticidad del emisor o receptor. Es decir, se deberán usar métodos para asegurar que el mensaje realmente haya sido enviado por quien dice haber sido enviado, y que fue recibido realmente por quien debió haber sido recibido.

- **No-rechazo:** Este es un concepto parecido al de autenticidad, ya que busca que el emisor no pueda rechazar el envío del mensaje. Éste en particular, es muy importante en aplicaciones de comercio electrónico, ya que en teoría el comprador no debería poder negar que realizó la autorización de su compra.

- **Disponibilidad:** Este concepto está más asociado con usabilidad, ningún criptosistema deberá sacrificar su funcionalidad por su seguridad. En otras palabras, todo usuario que tenga cumplidos los requisitos necesarios del criptosistema, siempre deberá poder recuperar la información que le corresponda. Hay veces que los sistemas se vuelven tan seguros, que cierran por completo el flujo de información entre sus usuarios.

Estas cualidades serán consideradas óptimas y se utilizarán para analizar a mayor profundidad la seguridad de los criptosistemas que son utilizados hoy en día en los sistemas de comunicación de redes inalámbricas.

1.2. Criptografía en la historia

Se considera que hace más de cuatro mil años, se escribió el primer parrafo en la historia de la Criptografía. En una ciudad cercana al río Nilo, llamada Menet Khufu, un maestro escribano plasmó con jeroglíficos la historia de la vida de su maestro. No usó un sistema de escritura secreta como ahora el mundo los conoce, tampoco usó un código de sustituciones de todos los jeroglíficos. Simplemente talló en la tumba del noble Khnumhotep II una serie de inusuales símbolos jeroglíficos en lugar de los ordinarios de la época. La mayoría de estos reemplazos fue realizada en las últimas veinte columnas de las doscientas veintidós. Esta sección habla acerca de los monumentos erigidos por Khnumhotep en servicio del faraón Amenemhet II. Probablemente, la intención de las sustituciones no fue la de complicar u obscurecer la lectura, si no de la de expresar el respeto y la autoridad que tenía el hombre noble. O tal vez, el anónimo escribano buscaba justamente lo que consiguió: Impresionar a sus lectores miles de años después. Aunque la inscripción no fuera secreta, aquí se tiene el primer indicio de uno de los elementos principales de la criptografía: La transformación deliberada de la escritura.

Se han hecho descubrimientos en el río Tigris de que en 1500 a.C. los mesopotámicos usaban piedras cuneiformes para grabar mensajes con substitución de caracteres. En arcilla escribían sus mensajes cifrados y la dejaban secar al sol. Una vez seca, era encapsulada en otra tableta de arcilla que servía de sobre. En cuanto llegaba a su destino, el receptor rompía el sobre de arcilla para descubrir el mensaje. En China se habla de una técnica parecida en la que usaban pasteles para esconder mensajes que pudieran pasar la guardia del emepreador. Se dice que las ahora famosas galletas de la fortuna, son la versión occidental de esta leyenda.

Esparta fue la primera cultura griega en utilizar un sistema de criptografía militar. En el siglo V a.C. usaban un dispositivo llamado "Escítala"para enviar mensajes secretos y comprobar que el emisor fuera del mismo grupo. El dispositivo consiste en una vara de madera alrededor de la cual se enrolla una cinta de papel o piel. Sobre esta cinta se escribe el mensaje a lo largo de la vara de madera. De tal manera de que cuando la tira es desenrollada, el mensaje se oculta hasta que vuelve a ser enrollada, otra vez, en una vara del mismo grosor. El historiador Tucídides y Plutarco, cuentan que estos dispositivos servían para comunicar a la milicia Espartana.

En India, el antiguo tratado económico, político y militar conocido como Artha-sastra (siglo III a.C.), pide que la comunicación con los espías del servicio de espionaje de India, sean contactados a través de escritos secretos. Sin embargo, uno de los más interesantes usos que ha tenido la criptografía es el recomendado en el libro erótico del Kama-sutra. Adjudicado a Vasyanyana, este libro enumera a la "Escritura Secreta" como uno de los sesenta y cuatro artes o yogas que las mujeres deberían estudiar y dominar. Dentro de la lista, tenemos cosas como: cantar, dar masajes, cocinar, etc. Pero lo que es curioso el arte cuarenta y cinco, conocido como "Mlecchita-vikalpa" que les ayuda a las mujeres establecer los detalles de sus encuentros con sus parejas. La técnica sugerida consiste en la sustitución

o el reacomodo de las letras del alfabeto.

Pero el más famoso de los criptosistemas clásicos, es el que hoy se le atribuye a Julio César. Suetonio cuenta que el César le escribía a Cicerón y a otros de sus amigos en un alfabeto cifrado. El cual consistía en recorrer tres letras del alfabeto, de tal manera que en vez de escribir la letra "A", se escribía la "D". En vez de la letra "B" se usaba la "E". y así sucesivamente hasta cubrir todas las letras. Hoy en día, todos los cifrados que usan el concepto de recorrer letras, son llamados "Cesar".

En la religión, tampoco faltó la criptografía. Por ejemplo, los Yazidi son una secta religiosa controversial cuyos libros sagrados se encuentran cifrados por el temor a la persecución de sus vecinos islámicos. Incluso el mismo Viejo Testamento en Hebreo, encubre la palabra "Babel"[1]intercambiando la última por la primera letra, la segunda por la penúltima, hasta esconder toda la palabra.

1.3. En busca de una comunicación segura

La criptología es el estudio de las comunicaciones través de canales inseguros y todos los problemas que se relacionan con ello. La criptografía se encarga de todo el proceso de diseñar sistemas, técnicas y mecanismos que protejan los datos para esta comunicación. Y el criptoanálisis se dedica a tratar de exponer fallas y buscar maneras de romper dichos mecanismos. En esta tesis se tendrán en cuenta estos tres términos para evaluar la seguridad en redes inalámbricas.

1.3.1. Una comunicación segura

Los algoritmos modernos para cifrar o descifrar de manera criptográfica se dividen en dos grandes clases:

- Llave Simétrica.
- Llave Pública.

Los algoritmos de llaves simétricas, se basan en el hecho de que tanto emisor como receptor comparten llaves para cifrar y/o descifrar sus mensajes, sin embargo esto implica que el emisor y receptor debieron tener un canal seguro de comunicación para ponerse de acuerdo en las llaves que van a utilizar en este ejemplo.

Se supondrá que Ale y Bob se encontraron en un pasadizo secreto al interior de una cueva en las afueras de la ciudad, donde en un papel anotaron la clave, la leyeron, la memorizaron y la quemaron; y nunca nadie se enteró de dicha junta y mucho menos de dicha clave.

Ahora, nótese la imagen **(agrégale referencia de diagrama)** donde Ale utiliza la llave para cifrar su mensaje, en seguida se lo envía a Bob a través de cualquier medio.

[1]En Jeremías 25:26 y 51:41, la palabra es sustituida por "SESHACH"

Bob recibe el mensaje cifrado y utiliza la llave recuperar el mensaje original. Y éste es el principio básico de los sistemas criptográficos clásicos, pero también de varios de los modernos como: AES, DES, RC4, etc.

Los algoritmos de llave pública fueron introducidos en 1970 y dan un enfoque completamente distinto que da solución al siguiente problema:

Supongamos que Ale y Bob se encuentran muy distantes y necesitan comunicarse de manera segura, sin embargo no tienen una llave para cifrar sus conversaciones y tampoco tienen un medio seguro para ponerse de acuerdo en una.¿Cómo pueden lograr Ale y Bob entablar una comunicación cifrada y segura?

Una manera de lograrlo sería la siguiente:

Bob tiene una caja fuerte, y solamente Bob conoce la combinación para abrirla. Bob envía la caja fuerte **abierta** a Ale. Cuando la recibe, Ale deposita un papelito con su mensaje, cierra la caja, gira abruptamente la rueda de las combinaciones y la envía de vuelta a Bob. Bob la recibe y abre la caja fuerte para recuperar el mensaje.

Este es el principio general que siguen todas las implementaciones de algoritmos de llave pública, tales como RSA, ElGamal, NTRU, McEliece, el de Cid, etc. Lamentablemente, un problema general que se puede encontrar sería el siguiente:

Suponga que Eva quiere conocer lo que Ale le está mandando a Bob, entonces intercepta el envío de Bob y reemplaza la caja fuerte por la suya, Ale la recibe sin siquiera notarlo, confiadamente deposita el mensaje en la caja fuerte de Eva y regresa el paquete. Eva recupera su caja fuerte y el mensaje de Ale.

Este tipo de problemas son generales a cualquier tipo de sistema criptográfico y se utilizarán en capítulos próximos para tratar de conseguir la llaves de cifrado o los mensajes enviados entre Alicia y Bob.

En su tiempo, los algoritmos de llave pública revolucionaron la criptografía, ya que representa lo que podría ser el último paso de una interesante progresión histórica. Al principio, la seguridad de la criptografía se basaba en mantener el método de cifrado en secreto.

Después, se asumía que el método era conocido pero había que mantener la llave (simétrica) completamente en secreto. Con la criptografía de llave pública, el método y la llave de cifrado son públicas, más aun, el método para conseguir la llave para descifrar es algo que hasta Eva conoce; sin embargo la seguridad reside en que, por ahora, conseguir esa llave **no** es computacionalmente posible.Y es que paradójicamente, a medida que avanza la capacidad computacional para conseguir dicha llave, aumenta también el poder de los algoritmos criptográficos.

Es importante mencionar, que teóricamente se espera un cambio de paradigma tanto computacional como criptográfico. Ya que la esperada invención de las computadoras cuánticas, traería consigo una solución inmediata a la dificultad computacional de factorizar grandes números enteros. Y es que este nuevo tipo de algoritmos garantizan que esta operación se vuelve tan sencilla como la suma de dos enteros. Afortunadamente, de igual manera ya hay propuestas criptográficas que bajo este mismo paradigma, prometen ser

completamente seguras.

Regresando a la era en la que los algoritmos de llave pública siguen siendo reinando la tierra, es importante notar el costo computacional que implican llega a ser tan grande que da paso a muchos de los algoritmos de llave simétrica para ser los que más populares en muchas de las aplicaciones que necesitan cifrado.

Por ejemplo:

Un canal de televisión decide transmitir una señal a través de internet , pero necesita que dicha señal vaya cifrada para proporcionarles sólo a sus clientes VIP los servicios de: alta definición y una gran velocidad de transferencia.

Esta situación excluye en primera instancia a los algoritmos de llave pública, pues la cantidad de tiempo que le toma cifrar y descifrar los paquetes de la transmisión de alta definición, van a hacer que sin importar que tan alta sea la velocidad de transferencia, la novela de la tarde sea imposible de ver pues el costo de procesamiento sería increíblemente alto. Y es por este motivo que en estos tiempos, los cifrados con llave pública se realizan sólo en situaciones donde cantidades pequeñas de datos son procesadas, como firmas digitales o incluso, la mejor aplicación, para establecer llaves simétricas seguras.

En el capítulo anterior, se vio que el protocolo 802.11 exige se expliquen los algoritmos de llaves simétricas. En particular se mencionaron dos grandes grupos a tratar:

- **Cifrado de Flujo:** para la implementación del ARC4.
- **Cifrado de Bloque:** para la implementación de AES y dos modos de cifrado de bloque: CTR y CBC.

Por lo que las siguientes secciones tratarán de explicar su funcionamiento general

1.4. One Time Pad

Esto cierra el capítulo.

1.5. Cifrado de Flujo

Este sistema busca cifrar bajo llave simétrica un flujo de información constante. Esto lo logra aplicando una transformación a los dígitos individuales del texto plano. Más a detalle, se tiene un mensaje m en texto plano el cual se puede expresar como una secuencia de dígitos, $m = m_0 m_1 ... m_{n-1}$, lo que se busca es transformar el mensaje en el texto cifrado $c = c_0 c_1 ... c_{n-1}$; para lograr esto se parte de un *flujo de llaves* $k = k_0 k_1 ... k_{n-1}$, las cuales son escogidas, en un principio, completamente aleatorias.

Ahora definamos la operación XOR, o disyunción exclusiva. Entonces se puede se puede llegar al mensaje cifrado simplemente realizando una operación de disyunción exclusiva[2]

[2]Este operador $\oplus$ también conocido como "O exclusivo" da la siguiente fórmula $a \oplus b = 1$ si $a \neq b$ con $a, b \in Z_2$

entre los bits del flujo de llaves y el mensaje en texto plano. Es decir, $c_i = m_i \oplus k_i$ para $0 \leq i \leq n-1$. A este algoritmo de cifrado se le conoce por el nombre de *Cifrado Vernam*, inventado por el Ing. Gilbert Vernam. Este cifrado también se conoce por el nombre de "One-time pad (OTP)", cabe recalcar que este cifrado es el único que se ha probado ser *"perfecto"*, en el sentido que es completamente seguro e imposible de romper.

Lamentablemente, a pesar de ser una excelente idea, y de ser teóricamente absolutamente seguro, ha habido casos donde la implementación de este algoritmo no ha sido buena, pues las llaves no han sido del todo aleatorias. Y es que la seguridad de este algoritmo depende de la independencia entre m y c, por lo que si se a través del criptoanálisis se pudiera encontrar cierta correlación entre ellos, es probable que se pudieran descifrar algunos mensajes, así mismo si se pudiera encontrar una relación entre las k_i's del flujo se podrían descifrar los mensajes siguientes.[3]

Esta idea general es la que buscan retomar todos los algoritmos de cifrado de flujo, la diferencia reside en los mecanismos para generar el flujo de llaves k. Usualmente se tiene un *Generador Psuedo-Aleatorio de llaves* que a partir de una llave más pequeña[4] genera el flujo de llaves k para cifrar el mensaje m. La gran ventaja de este cifrado es la gran velocidad con la que operan y generalmente son mucho más rápidos que los cifrados de bloque.

1.5.1. Clasificación

Considérese el estado del sistema criptográfico como los valores que toman las variables en un determinado momento. El principal problema implicará encontrar una manera de expresar el siguiente estado del sistema en términos del estado actual. Esta problemática divide los cifrados en dos tipos: Sincrónico y Asíncrono.

Sincrónico

Si el estado del criptosistema es independiente tanto del mensaje en texto plano m como del cifrado c, se dice que el cifrado es *sincrónico*. En este esquema cada bit de m es cifrado independientemente de los otros bits. Por lo tanto si se comete un error en uno de los bits, no se afectará el cifrado de los otros, a esta propiedad se le llama la de **No** propagación de errores.

A pesar de que esta propiedad pareciera deseable, trae consecuencia no tan deseables. Primero, la oportunidad de detectar un error durante el descifrado es reducida. Y segundo, un atacante tiene la posibilidad de realizar cambios controlados a ciertas partes del texto cifrado, lo que implicará cambios que pudieran llegar a cambiar todo el sentido del mensaje.

[3] En la historia ha habido ya un par de gobiernos que en una mala implementación de este algoritmo han sufrido las consecuencias. El problema reside en la dificultad de encontrar llaves generadas aleatoriamente.

[4] En el caso de WEP la llave compartida

Esto se implica que es necesario tener sincronizado el flujo de llaves k para proceder con el cifrado o descifrado. La sincronización usualmente se consigue incluyendo 'posiciones del marcador' en la transmisión. Produciendo que un bit de un bit del texto cifrado perdido durante la transmisión resulta en un descifrado incorrecto hasta que uno de los marcadores de posición es recibido.

Asíncronos

En contraste, los cifrado de flujo asíncronos tienen la facilidad de seguir descifrado correctamente incluso cuando el flujos de llaves pierde sincronía con el flujo de llaves del cifrado. Esto se debe a que el estado próximo del sistema está en función de algunos de los cifrados generados anteriormente.

Ahora, si se tiene que el cifrado de un bit depende de j bits cifrados anteriormente, entonces si el primer bit es recibido incorrectamente el descifrado de los siguientes j bits será incorrecto. Adicionalmente, el sistema es capaz de volverse a sincronizar y producir un cifrado correcto después de haber recibido correctamente los próximos j bits. Por lo que estos cifrados son una buena opción cuando la sincronización de los flujos de llaves es difícil de mantener.

Para este caso, el ataque de cambiar ciertos bits de mensaje m implican en el proceso un cambio y una posible detección. Pero como desventaja, un atacante conoce algunas de las variables para el generador de llaves pues se basa en el mismo texto cifrado. Dado que el algoritmo de cifrado que se utiliza en el cifrado WEP pertenece a los cifrados sincrónicos, no se verá más detalle de los asíncronos.

1.5.2. Tipos de Generadores

El gran problema con la implementación perfecta del cifrado de Vernam es el de generar llaves dichas llaves "aleatorias". Las principales propuestas acerca de estos generadores, son las siguientes:

- Generadores de congruencia.

  Los primeros sistemas utilizaban el concepto de generadores de números pseudo-aleatorios en vez del de flujos de llaves. Dichos generadores dan una secuencia de números x_i de la siguiente forma: $x_{i+a} = (ax_i + b) mod m$. Obviamente, se espera que el periodo de la secuencia sea grande y que m se conserve en secreto[5], se sugiere sea una potencia de dos y se tomen sólo los bits de mayor orden.

- Esquemas basados en Registro de Desplazamiento (Shift Register)

  La mayoría de los generadores de flujo de llaves se basan en algún tipo de Registro de Desplazamiento con Retroalimentación Lineal (LFSR). Esto se debe a dos razones

[5]Ya que si m fuera conocido sería muy sencillo resolver la ecuación para a y b con tan sólo dos números consecutivos dados.

principales: La clase de secuencias que se generan, normalmente cumplen los postulados de Golomb que se discutirán en la siguiente sección. Y la segunda es que el comportamiento de estas secuencias se puede analizar fácilmente a través del álgebra. Los dos principales registros son: el de Fibonacci y el de Galois. Basicamente consisten en un número de etapas numeradas de izquierda a derecha $0..n-1$ con retroalimentación para la etapa $n-1$ de todas las demás etapas. El contenido de las n etapas de un registro describe su estado. Dentro de esta categoría sólo por mencionar, caen los siguientes generadores: Combinaciones y filtros, multiplexor, controles de reloj, reducción y sumadores.

- Diseños alternativos Los que no entran en estas dos categorías, se consideran aquí:

  - SEAL

    Software-optimized Encryption Algorithm, se describe como una familia de funciones seudo-aleatoria de longitud creciente, donde se pueden generar fácilmente porciones arbitraras del flujo de llaves.

  - Técnicas de teoría de números

    Estos se basan en hacer diseños de generadores de llaves donde el predecir el flujo de llaves replica lo que se considera un problema 'difícil', como por ejemplo lo es el RSA, el logaritmo discreto, etc.

  - Otros esquemas Como por ejemplo: El generador $1/p$, que se basa en la expansión de esa fracción a una base b donde p y b son primos relativos. O también el generador de la mochila, que se basa en el problema de la mochila de investigación de operaciones, este problema es considerado 'difícil'. Además se combina con un algoritmo de desplazamiento. Por mencionar otros se tienen: cifrados al azar, autómatas celulares, PKZIP, etc.

  - RC4

    Rivest Cipher 4 fue diseñado por Ron Rivest en 1987, para RSA Data Security, Inc. Como su compañero de cifrado de bloque el RC2, RC4 es un cifrado con un tamaño de llave variable enfocado para el cifrado a granel. La simplicidad y el compacto tamaño del código de Ron junto con su gran velocidad de cifrado, han convertido al RC4 como el cifrado de flujo más utilizado. RC4 es considerado software confidencial

    Este algoritmo de cifrado es confidencial, sin embargo su "fortaleza" no reside en esta propiedad. Es más, el algoritmo con el que se trabaja realmente se llama ARC4 (Alleged RC4), esto se debe a que en una lista de correo, se publicó anónimamente dicho algoritmo. A pesar de que se conoce el algoritmo, la implementación que se utiliza sigue llamándose ARC4 pues el nombre de RC4 es marca registrada.

La descripción es simple. El flujo de llaves es independiente del texto plano, se manejan dos grandes algoritmos básicos, el algoritmo de generación seudo-aleatoria(PRGA) y el algoritmo de programación de llaves (KSA). El PRGA genera el flujo de llaves basado en el resultado del orden que genera el KSA. La gran diferencia de este algoritmo respecto a los otros, es que cuenta con una permutación aleatoria en la creación del flujo de llaves. El RC4 es utilizado en: SSH, SSL, TLS, IPSEC, WEP, etc. Por lo que se explicará paso a paso el funcionamiento de su implementación, el en capítulo propio de WEP.

1.5.3. Medidas Estadísticas

Se mencionó acerca de los postulados de Golomb cuando se mencionaron los cifrados basados en teoría de números. Estos postulados describen en palabras de su autor, la noción de *ensayos independientes*. Se quiere asegurar que aunque se conozca un valor previo de la sucesión, éste sea de ayuda para deducir el valor actual. Los postulados:

1. La cantidad de 1's en cada periodo, no debe de variar en más de uno de la cantidad de 0's.

2. En cada periodo, la mitad de las corridas debe tener longitud uno, un cuarto de ellas debe ser de longitud 2, un octavo debe tener longitud tres, etc. Mientras el numero de corridas exceda uno. Más aun, para cada longitud debe haber igual numero de corridas de 1's y de 0's.

3. Suponga que se tiene dos copias del la misma sucesión del periodo p desplazadas por una cantidad d. Entonces para cada d, $0 \leq d \leq p-1$ se puede contar el numero de coincidencias de las dos sucecciones A_d y el número D_d como la cuenta de los que no coinciden. El coeficiente de auto-correlación para cada d se define como $(A_d - D_d)/p$ y la función de auto-correlación toma tantos valores como d toma valores en su rango.

Una sucesión que satisfaga los postulados 1 y 3 se le conoce como una *sucesión-pn*, que en español se traduce a *Seudo Ruido*. Claramente estos postulados no son suficientes para considerarse una sucesión aleatoria, por lo que hay muchas pruebas estadísticas que se pueden aplicar a una sucesión para evaluar que tan bien ajustan que fueron generados por una fuente perfectamente aleatoria. Conceptualmente lo que se busca es comparar las sucesiones producidas por el generador, si dichas sucesiones no asemejan los comportamientos de una sucesión completamente aleatoria se descarta el generador. Sin embargo, incluso en el caso de generadores aleatorios se podría dar el caso de que se generen sucesiones catastroficamente débiles, por lo que es deber del generador que dichas sucesiones nunca se generen.

Con esto se cierra el módulo de cifrados de flujo y se retomará para el caso del Wired Equivalent Privacy, donde el RC4 es el algoritmo estrella del cifrado.

1.6. Cifrado por Bloques

A diferencia de los cifrados de flujo, los cifrados por bloques operan bajo una transformación fija en grandes bloques de datos de texto plano. Usualmente un cifrado de bloque toma dos elementos: una llave $k \in \{0,1\}^j$ y un mensaje $m \in \{0,1\}^n$ y produce un texto cifrado $c \in \{0,1\}^n$[6] Entonces la función del bloque de cifrado se puede ver como: $E : \{0,1\}^j x \{0,1\}^n \to \{0,1\}^n$

1.6.1. Modos de operación

Padding

ECB

CBC

CFB

OFB

CTR

1.6.2. AES

[6] La notación indica que son elementos binarios de longitud j y n

Capítulo 2

Criptosistemas informáticos

2.1. Distintos elementos

Aquí hacemos el diagrama del mundo de los criptosistemas

2.2. Cifrados Simétricos y Asimétricos

2.3. Cifrados de Flujo

2.4. Cifrados de Bloque

2.5. One way functions

Capítulo 3

Redes Inalámbricas

3.1. ¿Cómo funcionan?

Ese es un concepto general, sin embargo habrá que retomar ciertos conceptos más precisos de redes para después poder explicar los cifrados.

3.2. Pre-RSNA

3.2.1. ¿En qué consiste?

3.2.2. ¿Cual es su seguridad?

3.3. RSNA

3.3.1. ¿En qué consiste?

3.3.2. ¿Cual es su seguridad?

Capítulo 4

Fallas y Ataques

4.1. WEP

4.2. WPA/WPA2

4.3. Recomendaciones y conclusiones