Prospectivas Tecnológicas en el Ámbito Militar Para Integrar el Ciberespacio

Comandante Hugo Fernando Melgar Zúñiga, Fuerza Aérea de Perú

LA FINALIDAD DEL presente artículo es dar a conocer las prospectivas tecnológicas en el ámbito militar para integrar el ciberespacio, donde las NTIC (Nuevas Tecnologías de la Información y la Comunicación) han permitido el desarrollo vertiginoso de las redes de comunicaciones y la consecuente seguridad de la información. Estos sistemas de seguridad en la información y la comunicación brindan a las Fuerzas Armadas el necesario sostenimiento de las operaciones militares, y les garantizan superioridad en la libertad de acción, negando al adversario toda iniciativa y ventaja en la toma de decisiones.

Debemos tener presente que, desde el principio de la humanidad, siempre ha existido en el hombre la necesidad no solo de la comunicación sino de la protección de la misma, con el fin de evitar que la información sea conocida y divulgada. Hoy más que nunca, el poder que proporciona esta realidad es utilizado por los ejércitos en los campos de batalla, generando estrategias y tácticas a favor de una superioridad sobre el adversario y alcanzando un mayor desarrollo en los sistemas de información y en los canales de comunicación, teniendo como base las investigaciones científicas en el ámbito militar y el apoyo en los avances tecnológicos. Como consecuencia de estos logros, las instituciones militares por obvias razones, han buscado siempre protegerlos, primeramente por medio de técnicas de ocultamiento tales como mensajes cifrados y, posteriormente en el presente, con medios muchos más avanzados en materia de informática.

Siguiendo estos alineamientos, podemos afirmar que la guerra de la información tiene una estructura diferente a la guerra convencional, ya que utiliza el ciberespacio como campo de batalla en la identificación del enemigo, radicando allí una de sus fortalezas que con la introducción de las técnicas criptográficas, garantizan el éxito, y que puede materializarse en el lema siguiente expresado por el famoso estratega chino Sun Tzu: "Si conoces a tu enemigo y te conoces a ti mismo, no temas el resultado de una batalla. Si te conoces a ti mismo y no conoces a tu enemigo, por cada victoria ganada, sufrirás una derrota. Y, si no te conoces a ti mismo, ni conoces al enemigo, entonces sucumbirás en todas las batallas." [1]

Es de reconocimiento general que la criptografía en el ámbito militar es imprescindible y que su desconocimiento atenta gravemente contra la seguridad de las instituciones armadas. De allí se desprende que su relevancia parta no solamente de la robustez del algoritmo o del tamaño de la clave, sino de su implementación sistemática que garantice a su vez la efectividad en el nivel de seguridad, traducido en la protección del contenido de la información. El estudio de la criptografía requiere de fundamentos matemáticos complejos y su especialización demanda gran esfuerzo y dedicación, lo cual se logra después de muchos años de estudios y prácticas que requieren previamente del conocimiento de los aspectos básicos de la criptografía que es preciso profundizar.

Empleo de las redes de comunicaciones

La percepción existente sobre la baja velocidad de transmisión de datos en los Sistemas Satelitales, no solo es debido a la insuficiencia de la banda ancha que se asigna a las estaciones satelitales o a la complejidad de los aplicativos informáticos diseñados, sino al empleo de satélites geoestacionarios para las comunicaciones que al usar antenas fijas permiten que su orientación

no cambie, asegurando de esta manera, el contacto permanente con el satélite. Ello hace que los datos tengan que enviarse a una distancia aproximada de 36,000 km., donde se ubica la órbita de los satélites y que tenga que optarse por el empleo de una topología en red estrella, con doble salto satelital, lo cual ocasiona latencias que sobrepasan los 500 milisegundos (ms.), en comparación con las conexiones de banda ancha por fibra óptica, donde los datos pueden enviarse a un servidor a solo unas centenas de ms., debido a una distancia relativamente corta.

Para contrarrestar la latencia, las redes satelitales emplean una técnica llamada aceleración TCP (Transmition Control Protocol) o spoofing TCP, la cual consiste en "engañar" localmente al protocolo TCP, enviándole la confirmación de que los paquetes remitidos han llegado a su destino y que el envío de datos se lleva a cabo más cadenciosamente. Además, para eliminar el doble salto satelital, se emplean topologías en red malla, permitiendo que varias estaciones remotas puedan comunicarse entre sí a través de un único enlace, pasando por el satélite. Como consecuencia de esta implementación, no podemos desconocer que dichas mejoras tecnológicas incrementan los costos de mantenimiento, más aún cuando existe un incremento en la demanda de las redes satelitales.

Como resultado de los avances tecnológicos, el acceso a una red IP-VPN (Protocolo de Internet - Virtual Private Network), es posible en cualquier parte del mundo, siendo la INTERNET, la red IP con acceso más sencillo, en donde la conexión se obtiene generalmente a través de un módem de Línea de abonado digital asimétrica ADSL (sigla del inglés Asymetric Digital Subscriber Line). Esto se obtiene mediante el servicio de datos de un proveedor de telefonía móvil o del enlace a una red de área local (LAN) y con la exigencia de ciertos requisitos mínimos al enlace de comunicación. Lo recomendable es optar por un proveedor de redes IP de cobertura mundial, pudiendo estipularse una QoS (Quality of Service o calidad de servicio) en el marco de un SLA (Service Level Agreement, contrato de niveles de servicio), en regiones remotas o en lugares con una infraestructura débil, ya que en estos casos, el acceso a IP suele ser posible únicamente a través de una conexión satelital.

Una alternativa es el empleo de las redes IP-VPN encriptadas, las cuales otorgan niveles de seguridad esenciales para realizar enlaces remotos entre las dependencias que conforman las Instituciones Armadas. Estas redes deben satisfacer los máximos estándares de seguridad y cumplir con los principios fundamentales tales como: confiabilidad, simplicidad, seguridad, rapidez, oportuno, flexibilidad e interoperabilidad y garantizar el empleo de equipos criptográficos que permitan administrar las llaves y modificar el algoritmo de encriptación para el diseño de las Redes de Comunicaciones, que en su conjunto conforman un Sistema de Comunicaciones.

Empleo de la criptografía

Según el Diccionario de la Real Academia de la Lengua, la palabra Criptografía proviene de las raíces griegas kriptos que significa oculto, y graphos, que significa escritura, que al unirse traducirían, algo así, como escritura oculta y, que en nuestros días puede traducirse como el arte de escribir mensajes en clave o en secreto. Sin embargo, una definición más completa sería la siguiente: "Rama inicial de las Matemáticas y en la actualidad también de la Informática y la Telemática, que hace uso de métodos y técnicas con el objeto principal de cifrar, y por tanto proteger, un mensaje o archivo por medio de un algoritmo, usando una o más claves".[2] Pero podríamos sintetizar el concepto de la criptografía, como la ciencia que estudia los problemas de seguridad en la transmisión de la información por medio de un canal que se supone siempre inseguro, debiendo considerarse los principios criptográficos siguientes: la confidencialidad, la integridad de datos, la autenticación y el óptimo diseño de las Redes de Comunicaciones que garantice su seguridad, de manera que pueda ser factible la operatividad entre los diferentes Sistemas de Comunicaciones.

Haciendo historia, encontramos que la criptografía tuvo un rol preponderante en los acontecimientos de la Primera y Segunda Guerra Mundial, en donde la transmisión de los mensajes secretos se hacía efectiva con el fin de establecer las comunicaciones en el país, en el continente y con otros países al otro lado del océano Atlántico, y que trajo como efecto relevante el desarrollo de un vertiginoso avance de los sistemas criptográficos, tanto de las técnicas, como de las máquinas de cifrar. Dentro de este contexto, un hecho histórico trascendental narrado por David Khan, autor de la obra más completa sobre historia de la criptografía fue resumido de la forma siguiente: "Nunca un único criptoanálisis ha tenido tan enormes consecuencias"[3], referente a los hechos acontecidos el día 17 de enero de 1917, cuando el embajador de Alemania en Washington, Johann Von Bernstorff, recibió un telegrama del Ministro de Relaciones Exteriores alemán Arthur Zimmermann, en el que se podía leer una serie de instrucciones para la delegación germana en México, siendo interceptado y descifrado por los criptógrafos Nigel de Grey y William Montgomery de la Unidad de Inteligencia Naval Británica conocida como "Habitación 40". Precisamente, en ese telegrama, se anunciaba la guerra con los Estados Unidos, secreto que al ponerse al descubierto, cambió el rumbo de la historia, en vista de que los Estados Unidos ingresaba en la confrontación mundial y ayuda a los aliados, en miras a ganar la guerra.

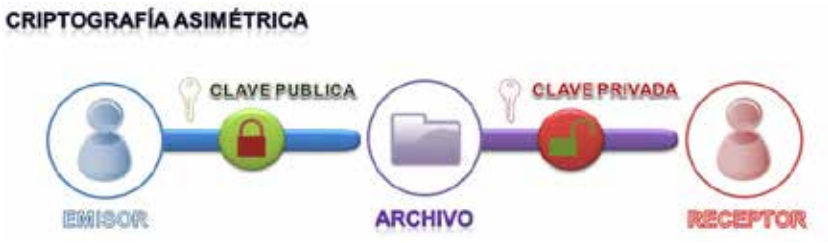
Como resultado del vertiginoso desarrollo de las NTIC y el uso masivo de las comunicaciones digitales, se ha producido un número creciente de problemas de seguridad, motivo por el cual, el objetivo de la criptografía se ha generalizado para estudiar las técnicas que se encargan de proporcionar seguridad a la información, pudiendo clasificar los criptosistemas como criptografía simétrica y criptografía asimétrica, cuyo concepción amerita un estudio más detallado.

Criptografía simétrica

También llamada criptografía de clave privada, la criptografía simétrica se usa para cifrar grandes cantidades de información de la manera más rápida y está conformada por el conjunto de algoritmos que tanto el emisor como el receptor emplean, mediante una sola llave (clave privada), con la finalidad de cifrar y descifrar el mensaje secreto, debiendo basarse la seguridad en la clave y no en el algoritmo usado.

Criptografía Asimétrica

También llamada criptografía de clave pública y está conformada por el conjunto de algoritmos que tanto el emisor como el receptor emplean, mediante dos llaves diferentes, con la finalidad de cifrar y descifrar el mensaje secreto. Como característica especial, la llave para cifrar mensajes se llama clave pública y puede ser conocida por todos, mientras que la llave para descifrar mensajes se llama clave privada y solo es conocida por un usuario, debiendo mantenerla en secreto, con lo cual el número de claves que emplea este criptosistema se determina por la cantidad de usuarios.

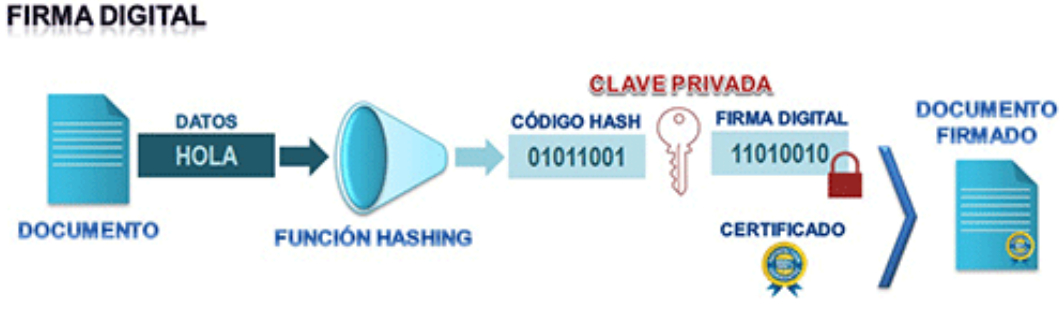


En la actualidad, la criptografía simétrica es ineficiente, en vista de que, al aumentar la cantidad de los usuarios, se incrementa el número de claves privadas en una proyección exponencial, con lo cual se dificulta la escalabilidad de dicho criptosistema. Por otra parte, es importante mencionar también que la criptografía asimétrica requiere más recursos para poder cifrar y descifrar un mensaje secreto, lo cual dificulta su empleo en el caso de archivos muy grandes, motivo por el cual se emplea una criptografía híbrida, donde el mensaje se envía en dos bloques: uno empleando la criptografía simétrica con el mensaje grande y otro utilizando la criptografía asimétrica solo con la clave privada, que descifra el mensaje largo, con lo cual se logra combinar la ligereza del algoritmo simétrico con la seguridad proveniente del intercambio de claves del asimétrico.

En el caso del Perú, con la aprobación de la Ley 27269 de mayo del 2000 referente a las Firmas y Certificados Digitales, se dió un paso trascendental en la regulación de las medidas técnicas de seguridad, que permiten el flujo permanente y seguro de datos e información a través de redes abiertas. Así lo estipula dicha Ley, en su artículo primero, según el cual: "Entiéndase por firma electrónica a cualquier símbolo basado en medios electrónicos utilizado o adoptado por una parte, con la intención precisa de vincularse o autenticar un documento, cumpliendo todas o algunas de las funciones características de una firma manuscrita."

Firmas y certificados digitales

Una de las aplicaciones criptográficas más importantes en la actualidad, son las firmas y certificados digitales, los cuales garantizan que las transacciones electrónicas sean seguras, brindando un clima de confianza a los usuarios que realizan operaciones de comercio electrónico por Internet, mediante la aplicación de un algoritmo matemático a los datos del documento, denominado función hashing. Posteriormente, al código hash resultante, se le aplica un criptosistema, empleando una clave privada con la finalidad de firmarlo digitalmente. Adicionalmente, se utilizan los servicios de una entidad que otorga certificados digitales llamada Autoridad de Certificación, cuya función es vincular la firma digital a los datos de verificación de un firmante y confirma su identidad, proporcionando una herramienta de gran utilidad para detectar la falsificación y la manipulación del contenido de un documento.



PROSPECTIVAS TECNOLÓGICAS

La criptografía moderna está basada en el segundo principio de Kerckhoffs, según el cual toda la seguridad debe descansar en la clave y no en el algoritmo; así como la computación digital trabaja en dos niveles de voltaje, donde un bit solo puede tomar valores de ceros (0) y unos (1), mientras que en la computación cuántica emplea el qubit (del inglés quantum bit, bit cuántico) cambiando el paradigma de los bits clásicos. De esta manera, un qubit, gracias a la superposición cuántica, puede no solo estar en uno de esos dos estados de 0 o 1, sino en cualquier combinación posible de ellos.

Las NTIC han permitido a la criptografía cuántica desarrollar técnicas que permitan establecer una comunicación segura entre el emisor y el receptor, empleando una clave secreta compartida, que puede ser usada como llave para cifrar y descifrar mensajes empleando métodos de criptografía simétrica; pero en la actualidad, su desarrollo es todavía experimental, según se describe en la siguiente cita: "El impacto de la computación cuántica sobre todo lo aplicado hoy en la criptografía es absolutamente catastrófico. Obliga a modificar todos los esquemas de seguridad informática y no solo se trata de cambios cualitativos (por ejemplo incrementar las dimensiones de las claves), sino que obliga a reformular cualitativamente las soluciones de reemplazo. Afortunadamente, la incipiente criptografía cuántica ha encontrado la forma de reemplazar los algoritmos de confidencialidad actuales por el sistema absolutamente inmune e inviolable del one-time-pad de Shannon".[4]

En un futuro cercano, cuando se construya una computadora cuántica, los principios de la criptografía moderna se desmoronarán, debido a que la mayor parte de los sistemas criptográficos actuales dependen de la complejidad matemática para factorizar números grandes, por no existir un algoritmo capaz de factorizarlo en un tiempo polinomial con las computadoras actuales. Por el momento, solo tenemos la teoría cuántica y los algoritmos cuánticos y los sistemas que existen son de cifrado cuántico.

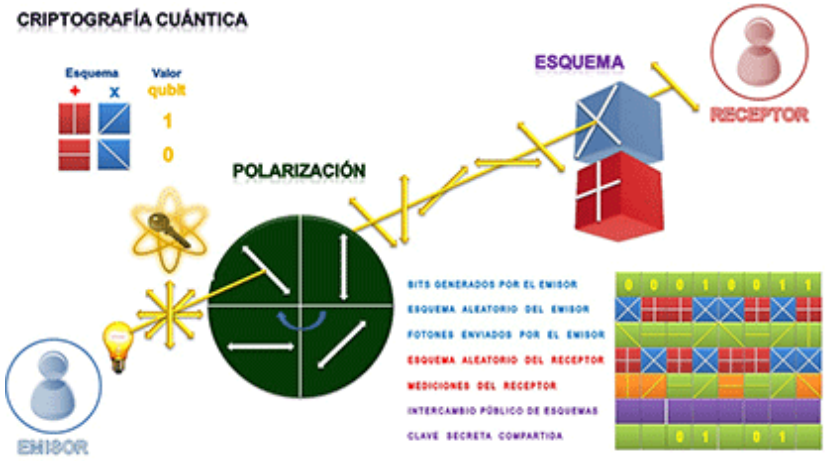
Criptografía cuántica

La seguridad de la criptografía cuántica se basa en la mecánica cuántica, a diferencia de la criptografía de clave pública tradicional que se basa en la complejidad computacional. Es por eso, que las actuales técnicas de la criptografía cuántica permiten establecer una comunicación segura, tanto para cifrar y descifrar mensajes secretos, en donde el emisor de qubits posee cuatro filtros de polaridad disponibles y el receptor de qubits posee dos filtros de polaridad disponibles de doble hendidura. Con base en lo anterior, se concluye que para realizar un sistema de cifrado cuántico, es necesario efectuar los procedimientos siguientes: el emisor comienza a transmitir una secuencia bits de 1 y 0 alternando los esquemas + y x en forma aleatoria; entonces, el receptor recibe alternando los esquemas + y x al aza. Posteriormente, el emisor y el receptor intercambian la sucesión de esquemas empleados y finalmente, usando solamente los bits de esquemas idénticos tanto del emisor como del receptor, se definirá la sucesión aleatoria de bits que servirá como clave secreta para las transmisiones futuras. Por lo tanto, si un intruso intenta obtener información de los fotones, existe una alta probabilidad de que la secuencia de bits del emisor y del receptor no coincidan. También pueden usarse funciones de hash para comprobar la integridad de la clave.

REFLEXIONES

El nuevo escenario estratégico global ha implicado que las nuevas amenazas tengan un carácter más regional y una naturaleza más variada. Como consecuencia, cualquier hecho aislado tiene connotaciones que pueden afectar el funcionamiento de las instituciones económicas, sociales y

culturales, incluso a nivel mundial. Las Nuevas Tecnologías de Información y la Comunicación (NTIC) están cambiando la forma de conducir las operaciones militares, implicando, de hecho, una transformación radical de los tradicionales escenarios de batalla, e incorporándose dos nuevos, el espacio y el espectro de la información.



Para facilitar el complejo y difícil ejercicio del mando, los responsables deben disponer de personal, organización, método y medios, que conformen lo que, dentro del campo profesional, se conoce habitualmente, como sistemas de Comando, Control, Comunicaciones, Computación, Inteligencia, Vigilancia y Reconocimiento (C^4IVR), y que en el más alto nivel de la OTAN se identifica como C3 como requerimiento para ejercer las funciones de comando, consulta y comunicaciones. Sin embargo, a pesar de tantas siglas que se han ido incorporando, estas funciones conforman, en esencia, un sistema C2 (Comando y Control).

Con la finalidad de poder conocer e identificar las Nuevas Tecnologías de Información y Comunicaciones (NTIC) que han permitido el vertiginoso desarrollo de aplicaciones criptográficas en el ámbito militar y que deben ser empleadas por los ejércitos en el Comando, Control, Comunicaciones, Computación, Inteligencia, Vigilancia y Reconocimiento (C^4IVR), es necesario hacer una retrospectiva histórica a los acontecimientos de la Primera y Segunda Guerra Mundial, referente a la información secreta que se transmitía en forma cifrada y que, tras ser interceptada por el enemigo, fue criptoanalizada, desencadenando el cambio, el curso de los acontecimientos y el desequilibrio unilateral de la balanza.

Los avances de la criptografía se han desarrollado, gracias al acrecentamiento de los conocimientos matemáticos y al uso militar que se le ha dado, por lo cual, la complejidad de los cifrados se ha incrementado, en vista de que a lo largo de la historia de las naciones, la obtención de información, su empleo, así como su protección y seguridad criptográficas son factores críticos en la estrategia del C^4IVR y en la inteligencia, respecto a la toma de decisiones importantes para la conducción de la política internacional y la defensa nacional.

El concepto de Guerra de Información que es un concepto relativamente nuevo en el cual se basa la guerra moderna, surgió de la combinación de varios factores, en donde el aprovechamiento de las NTIC para lograr la superioridad de la información, en apoyo a la estrategia militar nacional, ha jugado un papel preponderante, afectando el secreto de las comunicaciones del

adversario, mientras se refuerza y se protegen los propios sistemas de información. Curiosamente, este concepto estuvo presente en los orígenes del ser humano como respuesta a la necesidad de intercomunicación, y que posteriormente, bajo la figura de seguridad criptográfica, ha sido introducido por los ejércitos, en la protección de sus estrategias y tácticas frente al enemigo, siendo este binomio, la materia prima en todo proceso de Inteligencia y desarrollo de actividades.

Dentro de una visión futurista pero realista, el empleo de la criptografía cuántica en el ámbito militar nos permitirá transmitir información de manera segura, apoyándose en las leyes de la física, por contraposición a los métodos convencionales, normalmente basados en problemas computacionalmente difíciles. Lógicamente, el logro de estos resultados se fundamentará en la integración de la física cuántica con la criptografía, constituyéndose así en uno de los aspectos básicos y fundamentales de este sistema que busca proteger la transmisión de información, a través de la distribución de claves secretas.

En la actualidad, las NTIC permiten soluciones criptográficas eficientes, teniendo en cuenta que, empleando tecnologías abiertas, logran integrar la voz, data y video en un solo equipamiento criptográfico, bajo una plataforma IP que, a su vez, permiten soluciones ampliables, orientadas hacia el futuro. En el presente, estas tecnologías son empleadas por las Fuerzas Armadas a nivel mundial, con la finalidad de lograr una interoperabilidad de sus diferentes redes de comunicaciones, al fusionar sistemas de diferente tecnología y fabricación, sin perder la seguridad y garantizando plataformas unificadas de comunicaciones. Este equipamiento debe ser considerado como un aspecto importante y un criterio inflexible a considerar al momento de diseñar las aplicaciones criptográficas y las NTIC en el ámbito militar con el fin de impulsar y fortalecer el desarrollo del C^4IVR. ❑

Notas

1. Sun Tzu. El arte de la guerra; los trece capítulos. Versión española de la traducción francesa de Amiot de Esteve Serra (colección Los Pequeños Libros de la Sabiduría). Barcelona: José J. de Olañeta, 2005
2. Dr. Jorge Ramió Aguirre, Libro Electrónico de Seguridad Informática y Criptografía, Universidad Politécnica de Madrid, España, Sexta Edición 2006, página 39.
3. Khan, David, "The Codebreakers. The Story of Secret Writing", Macmillan Publishing Company, New York, 1967, pp. 266 ss. y 282 ss.
4. Hecht, Juan Pedro. Fundamentos de Computación Cuántica, para su aplicación en la teoría de la información cuántica y criptografía cuántica, Edición 2005, página 33.
22. Para ser justos, el programa Dassault "Gran Duc" francés es realmente anterior al F-40, al haber sido una contraparte del programa de UCAV original de la Agencia de Proyectos de Investigación Avanzada de Defensa—el abuelo del F-40.

El Comandante Hugo Fernando Melgar Zúñiga, Fuerza Aérea de Perú tiene los Títulos Profesionales de Ingeniero de Sistemas de la Universidad Nacional San Agustín e Ingeniero Electrónico de la Universidad Alas Peruanas, es egresado de la Maestría y del Doctorado en Ingeniería de Sistemas de la Universidad Nacional Federico Villarreal, obtuvo el Emblema de Honor por el primer puesto en el Programa de Estado Mayor en la FAP (2010), Diploma de Primer Puesto del Curso Básico de Inteligencia Aérea en la FAP (2002), Certificado de Primer Puesto en el Curso de Cisco Certified Networking en los Estados Unidos (2007) y el Diploma de Primer Puesto en el Curso de Seguridad Teleinformática y Criptografía en la República Argentina (2012).