Nombre del alumno: Johanne Joaquín Arriaga Díaz

Nombre del profesor: Icel Bernardo Lepe Arriaga.

Nombre del trabajo: Cuadro sinóptico de unidad III.

Materia: Redes de computadoras III.

Grado: Séptimo cuatrimestre.

Grupo: ISC13SDC0119-F

Frontera Comalapa, Chiapas a 13 de octubre de 2021

- Algoritmos de clave pública y firmas digitales
  - El algoritmo RSA
    - Algoritmo RSA un método de encriptado de datos algoritmo, muy usado hoy día para la transmisión segura de datos a través de canales inseguros.
      - Anillo de los enteros MD
        - Un concepto del que se parte es la existencia de un conjunto llamado de los números enteros, en el que está definida una relación de orden total (ser mayor que) y unas operaciones aritméticas (suma y producto, con las definiciones usuales) que le confieren estructura de anillo.
      - Conceptos básicos de aritmética en z
        - División enteraDados a, b ∈ Z, diremos que la división de a entre b tiene cociente q y resto r si es cierto que a = bq + r, siendo q un número entero sin restricciones, y r un numero ´ entero comprendido entre 0 y b − 1.
  - Otros algoritmos de clave pública
    - Cifrado de clave pública (o asimétrica): se basa en el uso de una pareja de claves, pública y privada, de las cuales una se usa para cifrar y la otra para descifrar, ambas relacionadas por una función trampa, suele ser una función matemática. Las claves se calculan usando la función y la inversa de ésta, siendo la función inversa la función trampa al ser muy difícil o imposible de calcular.
      - Algoritmo de Diffie-Hellman
        - Un protocolo para realizar el intercambio de claves. No es un cifrado, se creó para solucionar el problema de los cifrados de clave privada (o simétricos) en el intercambio de claves.
      - * Función irreversible x ∈ A, f(x) fácil de calcular y ∈ f(A), x = f-1 (y) difícil de calcular
      - * Función trampa x = f-1(y) Es calculable conociendo la trampa de la función. Pero sin conocer dicha trampa, y = f(x) es unidireccional. Además la trampa sólo se puede calcular con la clave privada.
  - Firma de claves simétricas
    - La criptografía de clave pública ofrece un método para el desarrollo de firmas digitales para verificar la autenticidad del origen de la información, y verificar que no ha sido modificada. Así ofrece el soporte para la autenticación e integridad de los datos, así como para el no repudio en origen, ya que el originador de un mensaje firmado digitalmente no puede argumentar que no lo es. Una firma digital es imposible de falsificar mientras no se descubra la clave privada del firmante.
      - Descifrado
        - La firma sólo puede ser descifrada utilizando la clave pública asociada. Asi, se tiene la seguridad de que el mensaje que ha podido descifrarse utilizando la clave pública sólo pudo cifrarse utilizando la privada. La firma digital, por tanto, es un cifrado del mensaje que se está firmando, pero utilizando la clave privada en lugar de la pública.
      - Funciones hash
        - Para evitar lentitud. Es una operación que se realiza en un conjunto de datos de cualquier tamaño para obtener otro conjunto, también denominado resumen de los datos originales, de tamaño fijo e independiente el tamaño original que, además, tiene la propiedad de estar asociado unívocamente a los datos iniciales, es decir, es prácticamente imposible encontrar dos mensajes distintos que tengan un resumen hash idéntico.
  - Firmas de claves públicas
    - Criptografía que se basa en una función de un sólo sentido. Significa que el cálculo de la función en un sentido es relativamente sencillo, pero, para deshacer ese cálculo, el coste computacional es muy alto.
      - RSA.
        - Se apoya en el problema de la factorización de números muy grandes al que, por el momento, no se ha encontrado una solución eficiente. Para generar dos claves RSA pública y privada, es necesario elegir dos números primos p y q para después multiplicarlos. De esta forma tenemos que N = p · q.
  - Compendios de mensajes
    - Dado m ∈ Z , m> 1, se dice que a, b ∈ Z son congruentes módulo m si y sólo si m|(a-b). Se denota esta relación como a ≡ b (mod m). m es el módulo de la congruencia. Es importante darse cuenta de que si m divide a a-b, esto supone que ambos a y b tienen el mismo resto al ser divididos por el módulo m. Ejemplos: 23≡2 mod 7 (porque 23=3.7 + 2), y -6≡1 mod 7 (porque -6= -7.1 +1)
      - La relación de congruencia como equivalencia. El conjunto de residuos. La relación de congruencia módulo m es una relación de equivalencia para todo m ∈ Z. Es decir, cumple las propiedades reflexiva, simétrica y transitiva. Como en toda relación de equivalencia, podemos definir el conjunto cociente de las clases de equivalencia originadas por la relación de congruencia. En este caso la relación clasifica a cualquier entero a según el resto obtenido al dividirlo por el módulo m.
        - Llamaremos Zm al conjunto cociente de Z respecto de la relación de congruencia módulo m. A la clase de equivalencia de un elemento a ∈ Z se la denota por [a]m o simplemente [a]. Para todo a∈Z se tiene que [a] = [r] en Zm, donde r es el resto de dividir a entre m. Por lo tanto, el conjunto Zm es finito y tiene melementos: Zm = { [0]m, [1]m, ... , [m-1]m}, donde la clase [i]m representa al conjunto de todos los enteros que son congruentes con imod m. A este conjunto cociente se le conoce como el conjunto de restos o residuos (módulo m)
        Ejemplo: siguiendo con el ejemplo anterior, está claro que en Z7, el número entero 9, el 16 y el 23 pertenecen todos a la clase [2], y que el entero -6, el 1 y el 8 pertenecen a la clase [1] Compatibilidad de la relación de congruencia con la suma y el productoSean m ∈ N y a, b, c, d ∈ Z tales que a ≡ b (mod m) y c ≡ d (mod m). Entonces se cumple que:i. a + c ≡ b + d (mod m)
  - El ataque de cumpleaños
    - Se menciona que un algoritmo de hash como SHA-1 o MD5 se ha “roto”. En rigor, estos algoritmos no se “rompen” sino que se cuestiona su robustez en determinados supuestos, gracias al avance de las matemáticas.
      - “paradoja del cumpleaños”,
        - La función de probabilidad de nacimientos es uniforme (Es igualmente probable nacer en un día que en otro) la probabilidad es de 1/365, 25. Si planteamos cuantas personas en una habitación se necesitan para tener una probabilidad mayor del 50% de que dos de ella compartan cumpleaños, la respuesta es 23. Las influencias del clima y de las costumbres, la distribución de probabilidad de nacimiento no es uniforme y algunos meses (singularmente los que distan 9 meses de los de verano) computan más nacimientos que otros. De esta forma la probabilidad de que 2 personas en una sala llena de gente cumplan años el mismo día es bastante alta.
          - Asi la probabilidad de que dos documentos diferentes en una colección computen el mismo hash, el valor, , es significativamente mayor que 1/(2^numbits).

            Si los documentos con los que trabajamos son de tipo estructurado esta debilidad no es significativa. Pero, si trabajamos documentos con áreas modificables, la debilidad comienza a ser significativa, ya que un atacante podría modificar de forma ventajosa para él la parte del contenido modificable generando resultados que podrían resultar ser colisiones respecto al valor de hash del documento original.