UNIVERSIDAD AUTÓNOMA DEL ESTADO DE HIDALGO

"AMOR ORDEN Y PROGRESO"

ESCUELA SUPERIOR DE HUEJUTLA

LICENCIATURA EN CIENCIAS COMPUTACIONALES

Lectura

ALGORITMO DE FIRMA DIGITAL DSA

Presenta:

EDUARDO AGUIRRE HERNANDEZ

Materia:

CRIPTOGRAFÍA

Docente:

MTRO. VICTOR TOMAS TOMAS MARIANO

2018

Objetivo:

La presente lectura tiene como objetivo dar a conocer el funcionamiento del algoritmo DSA para firmar digitales, así como su aplicación, enfocado a alumnos interesados en el tema de la criptografía y las diferentes aplicaciones de esta.

Introducción

En el presente documento se explica el algoritmo *Digital Signature Algorithm* (DSA), los pasos para la obtención de la clave pública y clave privada que se utilizan posteriormente para firmar un archivo en forma digital.

Una firma digital es un análogo electrónico de una firma escrita para garantizar que el signatario reclamado firmó la información. Además, se puede usar una firma digital para detectar si la información se modificó o no después de que se firmó (es decir, para detectar la integridad de los datos en un archivo).

El proceso de firma digital se divide en 2 partes:

1. Generación de la firma (lado del emisor):

- Generar un par de clave pública y proporcionar clave por parte del remitente del mensaje.
- Generar el resumen del mensaje a partir una función hash.
- Generar la firma digital con el resumen del mensaje y con la clave privada.
- Enviar el mensaje, la firma digital y la clave pública al receptor.

2. Verificación de firma (lado del receptor):

- Generar el resumen del mensaje usando la misma función hash.
- Verificar la firma digital con el resumen de mensaje y con la clave pública.

En la figura 1 se muestra un diagrama del proceso de generación y validación de firma digital sobre un mensaje o archivo.

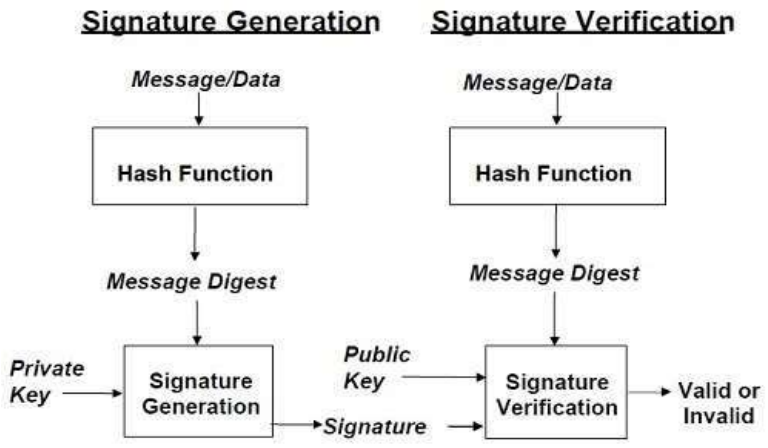

Fig. 1 Esquema generación y validación firma digital. Fuente [2].

Algoritmo de firma digital DSA

DSA es un estándar del Gobierno Federal de los Estados Unidos para firmas digitales. Fue propuesto por el instituto Nacional d Estándares y Tecnología (NIST) en agosto de 1991 para uso en su estándar de firma digital, especificando en FIPS 186 en 1993[2]. Las etapas del algoritmos DSA y los ejemplos que se describen a continuación están basados en los tutorías del Dr. Herong Yang [2].

1. La primera parte del algoritmo DSA es generar la clave pública y generar la clave privada, que se describe de la siguiente manera.

    a. Elegir un número primo q, que se llama divisor principal.
    b. Elegir otro número primo q, tal que p-1 mod q = 0. P se denomina módulo primo.
    c. Calcula un número entero g, tal que 1<g <p, g^q mod p = 1 y g = $h^{((p-1)/q)}$ mod p. q también se llama módulo de orden multiplicativo g de p.
    d. Elegir un número entero x, tal que 0<x <q.
    e. Calcular *y* como g^x mod p.
    f. Agrupamos nuestra clave pública como {p, q, g, y}.
    g. Agrupamos nuestra clave privada como {p, q, g, x}.

2. La segunda parte del algoritmo DSA es la generación y verificación de la firma, que se describe como:

    El lado del remitente debe realizar:

    a. Generar el resumen del mensaje, usando un algoritmo hash como SHA1, se conoce como “h”.
    b. Generar un número aleatorio k, tal que 0 <k <q.
    c. Calcular un número r como (g^k mod p) mod q. Si r = 0, selecciona una k diferente.
    d. Calcular un número i, tal que *k*i mod q = 1*. i se llama inverso multiplicativo modular de k modulo q.
    e. Calcular s = i * (h + r * x) mod q. Si s = 0, selecciona una k diferente.
    f. Agrupe la firma digital {r, s}.

3. Tercera parte, se verifica la firma de un mensaje:

    a. Generar el resumen del mensaje (h), usando el mismo algoritmo hash.

b. Calcular w, de modo que s * w mod q = 1. w se denomina inverso modular de s modulo q.
c. Calcular u1 = h * w mod q.
d. Calcular u2 = r * w mod q.
e. Calcular v = (((g^{u1}) * (y^{u2})) mod p) mod q.
f. Si v == r, la firma digital es válida.

Ejemplo para ilustrar el funcionamiento del algoritmo de firma digital DSA, con números pequeños primo q = 11 y módulo primo p = 23.

Algoritmo de firma digital DSA, Ejemplo 1.

- El proceso de generar la clave pública y la clave privada:

```
q = 11 # divisor principal seleccionado
p = 23 # módulo primario calculado: (p-1) mod q = 0
g = 4 # calculado: 1 < g <p, g^q mod p = 1:
            # 4^11 mod 23 = 1: 4194304 mod 23 = 1
x = 7 # seleccionado: 0 < x < q
y = 8 # calculado: y = g^x mod p = 4^7 mod 23
{23,11,4,8} # la clave pública: {p, q, g, y}
{23,11,4,7} # la clave privada: {p, q, g, x}
```

- Con la clave privada {p, q, g, x} = {23, 11, 4, 7}, el proceso para generar una firma digital con un valor hash de mensaje h = 3 es:

```
h = 3 # el valor hash como el resumen del mensaje
k = 5 # seleccionado: 0 < k <q
r = 1 # calculado: r = (g^k mod p) mod q = (4^5 mod 23) mod 11
i = 9 # calculado: k * i mod q = 1: 5 * 9 mod 11 = 1
s = 2 # calculado: s = i*(h+r*x) mod q = 9*(3 + 1 * 7) mod 11
{1,2} # la firma digital: {r, s} del mensaje y/o archivo
```

- El proceso de verificación de la firma digital {r, s} = {1, 2} con la clave pública {p, q, g, y} = {23,11,4,8} puede ilustrarse como:

```
h = 3 # el valor hash como el resumen del mensaje
w = 6 # calculado: s * w mod q = 1: 2 * 6 mod 11 = 1
u1 = 7 # calculado: u1 = h * w mod q = 3 * 6 mod 11 = 7
u2 = 6 # calculado: u2 = r * w mod q = 1 * 6 mod 11 = 6
v = 1 # calculado: v = (((g^u1) * (y^u2)) mod p) mod q
          # = (((4^7) * (8^6)) mod 23) mod 11 = 2
          # = 16384 * 262144 mod 23 mod 11 = 1
v == r # verificación aprobada
```

Algoritmo de firma digital DSA, Ejemplo 2

<table>
<tr><td>q = 7</td><td>p = (p-1) mod q = 0
p = 29</td></tr>
<tr><td>g = 1 < g < p
g^q mod p = 1
g = 23
23^7 mod 29 = 1</td><td>x = 0 < x < q
x = 3

y = g^x mod p
y = 16</td></tr>
<tr><td colspan="2">Clave pública {p, q, g, y} = {29, 7, 23, 16}</td></tr>
<tr><td colspan="2">Clave privada {p, q, g, x} = {29, 7, 23, 3}</td></tr>
<tr><td colspan="2">Función hash (v1- v2) *v3

<table>
<tr><td>V1</td><td>V2</td><td>V3</td><td>V1</td><td>V2</td><td>V3</td><td>V1</td><td>V2</td><td>V3</td><td></td></tr>
<tr><td>H</td><td>O</td><td>L</td><td>A</td><td></td><td>E</td><td>D</td><td>U</td><td>A</td><td>suma</td></tr>
<tr><td>72</td><td>79</td><td>76</td><td>65</td><td>32</td><td>69</td><td>68</td><td>85</td><td>65</td><td></td></tr>
<tr><td colspan="3">(v1- v2) *v3
-532</td><td colspan="3">(v1- v2) *v3
2277</td><td colspan="3">(v1- v2) *v3
-1105</td><td>640</td></tr>
<tr><td>R</td><td>D</td><td>O</td><td></td><td>U</td><td>A</td><td>E</td><td>H</td><td></td><td></td></tr>
<tr><td>82</td><td>68</td><td>79</td><td>32</td><td>85</td><td>65</td><td>69</td><td>72</td><td>32</td><td></td></tr>
<tr><td colspan="3">(v1- v2) *v3
1106</td><td colspan="3">(v1- v2) *v3
-3445</td><td colspan="3">(v1- v2) *v3
-96</td><td>-2,435</td></tr>
<tr><td colspan="9">SHA(M) = -1,795</td><td>-1,795</td></tr>
</table>

k = 0<k <q
k = 5</td></tr>
<tr><td colspan="2">r = (gk mod p) mod q
r = (235 mod 29) mod 7
r = 4</td></tr>
<tr><td colspan="2">i = k * i mod q = 1
i = Inverso (5,7)
i = 3</td></tr>
<tr><td colspan="2">s = i * (h + r * x) mod q
s = 3 * (-1795 + 4 * 3) mod 7
s = 6</td></tr>
<tr><td colspan="2">Firma digital
{r, s} = {4, 6}</td></tr>
<tr><td colspan="2"></td></tr>
</table>

w = s*w mod q = 1 Inverso (s, q) Inverso (6, 7) = 6
u1 = h * w mod q u1 = (-1795 * 6) mod 7 u1 = 3
u2 = r * w mod q u2 = (4 * 6) mod 7 u2 = 3
v = (((gu1) * (yu2)) mod p) mod q v = (((233) * (163)) mod 29) mod 7 v = 4 Si v = r La firma digital es valida Verificación aprobada

La función hash (h) está basado en el proceso descrito en [1], se observa que cada carácter del mensaje se le asocia el código ASCII para calcular el valor de “h”.

Conclusiones

La firma digital permite mantener la integridad de un mensaje o archivo de cualquier tipo, en los ejemplos presentados se comprueba las etapas del algoritmo DSA con resultados satisfactorios. Las pruebas con archivos de texto, en extensión docs, ppt, xls, pdf, mp3 e incluso video se lograron también firmar en forma adecuada y su verificación de integridad. El código fuente en lenguaje java se puede descargar de la referencia [2] en línea, las pruebas se realizan desde ventana de comandos, sin embargo, con mejoras del código fuente se puede adaptar una GUI con Netbeans.

Referencias

1. Aguilar M. E. (2012), Sistema tutorial de Fundamentos de Criptografía, Tesis de ingeniería en computación, UNAM.
2. Yang H., (2018), Cryptography Tutorials - Herong's Tutorial Examples, consultado el 05/10/2018, link: http://www.herongyang.com/Cryptography/DSA-Introduction-What-Is-Digital-Signature.html