Científica Vol. 12 Núm. 1 pp.31-37
© 2008 ESIME-IPN. *ISSN 1665-0654*. Impreso en México

Generador de identidades seudónimas

Bernabé-Humberto Nava-Correa
Rubén Vázquez-Medina
María-Elena García-León

Sección de Estudios de Posgrado e Investigación,
Escuela Superior de Ingeniería Mecánica y Eléctrica,
Unidad Profesional Culhuacán, Instituto Politécnico Nacional (IPN). Av. Santa Ana 1000, Edif. 2, 3er piso,
Col. San Francisco Culhuacán, 04430, México, DF.
MÉXICO.

correo electrónico: bnava@calmecac.esimecu.ipn.mx
mgarcía@calmecac.esimecu.ipn.mx
ruvazquez@ipn.mx

Recibido el 13 de febrero de 2007; aceptado el 3 de octubre de 2007.

1. Resumen

En este artículo se describe y analiza, para su implementación práctica, un sistema de generación de identidades seudónimas para usuarios que realizan transacciones comerciales a través de Internet sin poner en riesgo su privacidad y la confidencialidad de su información personal. Este sistema genera dos objetos para la identidad seudónima, uno es el usuario seudónimo y el otro es su credencial que lo acredita como miembro del sistema. Este sistema se basa en el modelo propuesto en 1999 por Lysyanskaya, Rivest y Sahai (Sistema Seudónimo LRS).

Palabras clave: autenticación, seudónimo, nym, privacidad, confidencialidad.

2. Abstract (Generator of Pseudonym Identities)

In this paper a pseudonym identity system is described and analyzed for its practical implementation. The pseudonym identity is defined for the Internet users, who make trade transactions with privacy and confidentiality guaranties. This system produces two objects: pseudonym user (nym) and credential and it is based in the model proposed in 1999 by Lysyanskaya, Rivest and Sahai (Pseudonym System LRS).

Key words: authentication, pseudonym, nym, privacy, confidentiality.

3. Introducción

La falta de privacidad es un problema real ante lo conveniente de Internet. Si no se tiene el debido cuidado en el manejo de la información personal, existe el riesgo de tener afectaciones económicas, sociales o personales (www.cert.org).

Hay varios métodos que aseguran la información que se transmite a través de Internet y la protegen de terceros (www.buzan.com.mx). Sin embargo, hay muchos usuarios que buscan tener alternativas adicionales que otorguen privacidad en el manejo de su información personal. Este requerimiento se puede satisfacer usando sistemas seudónimos. Chaum fue el primero en introducir los sistemas seudónimos en 1985 [1]. Un sistema seudónimo es un conjunto de elementos y técnicas que permiten a usuarios mantener protegida su identidad real e interactuar con múltiples organizaciones de forma "anónima" mediante el uso de diferentes seudónimos, vía Internet. Los sistemas seudónimos también son conocidos como "sistemas de seudónimo y credencial". Consisten de varias entidades tales como: autoridades de certificación, organizaciones de seudónimo y credencial, clientes, etcétera.

Una solución basada en sistemas seudónimos es útil debido a que Internet es una fuente muy amplia de recursos de información, comunicación, operaciones de negocios/ publicidad y venta de bienes y servicios. Internet está cambiando la cultura de la sociedad al romper los modelos tradicionales de hacer negocio, interactuar, capacitarse, etcétera.

Un sistema seudónimo requiere de una infraestructura tecnológica que implica una importante inversión en recursos humanos y materiales. Esta infraestructura debe considerar el diseño y la puesta en operación de protocolos seguros de comunicaciones. Sin embargo, en este artículo sólo abordamos la descripción y análisis del generador de identidades seudónimas; lo relativo a la infraestructura tecnológica de la red seudónima queda fuera del alcance de este trabajo.

Así, un sistema que genera identidades seudónimas tiene la finalidad concreta de otorgar privacidad a la información personal de un usuario de Internet. Con esto, un usuario puede

Tabla 1. Comparativa de sistemas seudónimos.

	Chaum & Evertse	Damgard	Chen	*LRS
Confianza y responsabilidad de la *AC	Amplia	Mínima	No confiable y mínima responsabilidad	Mínima
Técnica y seguridad	*RSA (fiable)	Construcciones de prueba de conocimiento cero (ineficaces)	Logaritmo discreto (fiable)	Problema del logaritmo discreto (fiable)
Compartir identidad	Sí	Sí	Sí	Sí
Definición de usuario	No	No	No	No
Análisis de tráfico	No protege	No protege	No protege	No protege

*LRS (Lysyanskaya, Rivest y Sahai)
*AC (Autoridad de certificación)
*RSA (Rivest-Shamir-Adleman)

proteger su identidad mediante el uso de un usuario seudónimo con el que se acreditará ante una instancia con la que previamente se registró. La identidad seudónima ayuda a reducir la cantidad de información personal sensible que se transmite por Internet, y con ello contribuye a reducir los riesgos de seguridad que un usuario pudiera tener si alguien captura y manipula dicha información.

Un ejemplo de esta situación lo encontramos en la nota que presenta Olivia Aguayo en el periódico *Reforma* (México) en febrero de 2007 [2]. En esta nota se hace referencia al hecho de que peligra la identidad de los usuarios de Internet, ya que información confidencial, tal como fotografías, domicilio, teléfono, etc., puede ser aprovechada por personas malintencionadas, quienes para lucrar publican dicha información sin consentimiento del propietario, poniéndolo en una situación muy incomoda y de alto riesgo a su seguridad personal, económica y familiar.

En su estado maduro, un sistema seudónimo procura evitar la rastreabilidad del usuario en una comunicación en línea, al tiempo que no revela su identidad real. Por ello se dice que estos sistemas otorgan al usuario garantías de seguridad, sin embargo, para un proveedor de productos y servicios en línea pudiera representar un fraude potencial. Pero es importante resaltar que no se trata de que los usuarios tengan una autenticación anónima, sino seudónima, lo que permite otorgar entonces garantías a ambas partes que se involucran en una transacción en línea. Por ejemplo, en caso de ocurrir algún ilícito, la organización emisora de la identidad seudónima puede establecer el enlace entre el usuario seudónimo y su identidad real. Por supuesto, esto solamente se haría si le es requerido a través de una orden emitida por una autoridad y con el conocimiento del usuario. Por lo tanto, un sistema seudónimo debe contribuir a consolidar la confianza del usuario al hacer uso de Internet, y debe ayudar a establecer una legislación en materia de protección de datos.

Aunque no es sencilla la implementación de un sistema seudónimo completo, resulta deseable tener herramientas que contribuyan a su implementación y entendimiento. De esta manera, en este artículo se describe, analiza y propone un generador de usuarios seudónimos y sus credenciales.

Como marco de referencia para este artículo, en la tabla 1 presentamos un resumen de los distintos sistemas seudónimos que se han desarrollado desde 1985. Como se aprecia en la tabla 1, todos los sistemas tienen el problema de no protección contra análisis de tráfico. Pero, el que tiene mejores características y considera el uso de protocolos seguros de manejo de información personal es el sistema seudónimo LRS. Por ello, el generador que proponemos para su implementación se basa en el modelo que emplea este sistema y se hace uso, además, de la teoría de números, en particular del problema del logaritmo discreto.

4. Desarrollo

Lysyanskaya, Rivest y Sahai (LRS) presentan un modelo de sistema seudónimo donde la identidad de un usuario es una noción bien definida [3]. En este sistema los usuarios tienen una postura a comportarse responsablemente; además de que en todo momento su identidad está protegida. El sistema LRS se basa en la presunción de que cada usuario tiene una llave pública cuya correspondiente llave privada sólo él conoce, y es favorablemente motivado a guardarla confidencialmente.

Esto implica que si, esta llave pública se registra como su llave de firma digital legal, el descubrimiento de su llave privada permitiría a otros forjar las firmas en los documentos legales o financieros importantes en su nombre. Ahora, si un usuario comparte su credencial debe compartir también su llave privada, lo cual va en contra de la premisa principal de confidencialidad de la llave privada, ya que hay riesgos directos sobre el propietario de la identidad seudónima y sus credenciales.

El generador de seudónimos y credenciales del sistema seudónimo LRS, consiste en protocolos criptográficos interactivos seguros, los cuales se basan esencialmente en el problema del logaritmo discreto. Por ello, a continuación damos su definición, y como complemento necesario damos también la definición del problema de Diffie-Hellman.

Se define el logaritmo discreto de un elemento β en la base α de G como el entero x en el intervalo $0 \leq x < n$, tal que

$$\alpha^x = \beta \tag{1}$$

se escribe:

$$x = \log_\alpha \beta \tag{2}$$

El problema del logaritmo discreto puede enunciarse como sigue: Dado un número primo p, un elemento primitivo de Z^*_p y un elemento $\beta \in Z^*_p$, encontrar un entero x, $0 \leq x < p-2$, tal que

$$\alpha^x = \beta \pmod p \tag{3}$$

Resolver este problema consiste en encontrar un método computacionalmente eficiente que encuentre logaritmos en el grupo dado [8]. Los recursos más utilizados para determinar logaritmos discretos se basan en los siguientes métodos [4]:

- Método de la búsqueda exhaustiva.
- Método del paso gigante-paso enano.
- Método de Pohlig-Hellman.

El problema de Diffie-Hellman es el mismo que para el logaritmo discreto.

La dificultad de computar logaritmos discretos en un grupo de orden primo, es una conjetura ampliamente creída. Suponga que se da un número primo q de k-bits y un número primo p tal que $q|(p-1)$. Por Z^*_p se denota el grupo multiplicativo módulo p. Permita a $g \in Z^*_p$ ser de orden q. Entonces g es un generador de un grupo de orden q, llamémoslo G_q.

Dado $g, h_1, h_2 \in G_q$ donde

$$h_1 = g^x \bmod p \tag{4}$$
$$h_2 = g^y \bmod p \tag{5}$$

se seleccionan aleatoriamente con distribución uniforme, es difícil calcular h_3,

$$h_3 = g^{xy} \bmod p \tag{6}$$

Con estos elementos procedemos a hacer una descripción del generador de identidades seudónimas que hemos desarrollado en una realización de *software* empleando MatLab™.

4.1 Descripción formal del sistema

En el sistema de generación de identidades seudónimas desarrollado se considera que existe una interacción, a través de un protocolo genérico, de dos entidades, el usuario y la organización. El usuario es quien solicita la obtención de una identidad seudónima. La organización es quien genera y otorga la identidad seudónima de los usuarios, a través de una entrevista directa o por medio de una comunicación a distancia realizada con garantías de confidencialidad y autenticidad, como las convencionales que existen en la actualidad que emplean mecanismos criptográficos que combinan algoritmos asimétricos y simétricos.

En la figura 1 se muestra un diagrama de bloques del sistema. Nótese que consiste en esencia de dos subsistemas, uno que genera la identidad seudónima y otro que genera la credencial asociada a dicha identidad. La salida de estos dos subsistemas es una sucesión numérica resultante de una combinación de las variables de entrada que representan la identidad real del usuario.

Generador del usuario seudónimo (nym)

Este subsistema es un protocolo que permite la generación del usuario seudónimo, también conocido como nym, el cual

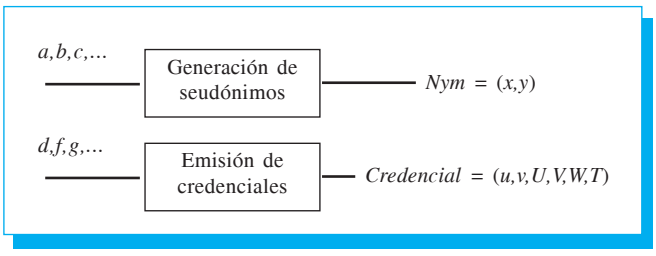

Fig. 1. Entradas y salidas genéricas del generador.

deberá tener asociada una credencial para poder completar la identidad seudónima del usuario solicitante. El protocolo de este subsistema consta de tres pasos, los cuales a continuación se describen:

1) Generación de la llave maestra de usuario:
- El usuario toma su llave maestra secreta $x \in Z^*_q$ y pública $g^x \bmod p$.

2) Generación de la llave credencial de la organización:
- La organización toma dos exponentes secretos, $s_1 \in Z^*_q$ y $s_2 \in Z^*_q$, y pública, $g^{s_1} \bmod p$, $g^{s_2} \bmod p$.

3) Generación del nym (véase a detalle después):
- Llave pública maestra del usuario U es g^x.
- Llave privada maestra del usuario U es x.

Generación del nym

En la figura 2 se muestra el protocolo para producir el nym correspondiente. Primero, a la entrada del generador se seleccionan al azar los números primos, q, p y g, donde q debe cumplir la condición $q \mid (p-1)$, limitando el valor de g $(0 < g < q)$ y así construir el conjunto de enteros de orden primo Z^*_q, del cual el usuario va a seleccionar al azar un valor x (llave privada), así como los posteriores que se seleccionen de este conjunto por ambas entidades. Después el usuario (U) realiza la operación del problema del logaritmo discreto, tomando el valor x obtenido, y envía el resultado a la organización generadora de seudónimos y credenciales (O). Enseguida la O selecciona dos números secretos del grupo de enteros Z^*_q, aplica el problema del logaritmo discreto en ambos y los envía al U. U cuenta con las llaves g^x ($K\text{púb}_U$) y x ($K\text{priv}_U$), de las cuales envía sólo la pública a O. U selecciona un número γ del grupo de enteros Z^*_q, para realizar la operación g^γ que define a $\tilde{a}$, y luego calcula $\tilde{a}^{K\text{priv}_U}$ que define $\tilde{b}$. Enseguida le envía $\tilde{a}$ y $\tilde{b}$ a O. O genera un número r del grupo multiplicativo módulo q de enteros y calcula $\tilde{a}^r$ que define a a y se la envía a U. U calcula $a^{K\text{priv}U}$ que define a b. Después U y O ejecutan el protocolo Π con los números a, b, $\tilde{a}$ y $\tilde{b}$. La ejecución del protocolo Π (prueba de igualdad de logaritmos discretos) permite asegurarse de que no hayan existido problemas durante el proceso. También permite de forma particular que el usuario esté en condiciones de autenticar a la organización y de igual forma la organización al usuario. El nym (N) es conocido por U y O (véase figura). Para autenticar el nym (a, b) es necesario correr un protocolo seguro por ambas partes, éste puede ser el mismo protocolo Π, pero en este caso consistiría de la siguiente igualdad

$$\log_a b = \log_a b \qquad (7)$$

Generación del Seudónimo

Entradas:

q es un número primo de k-bits.
p es un número primo de k-bits.
g es un número primo de k-bits.
se debe cumplir que: $q \mid (p\text{-}1)$.
se debe cumplir que: $0 < g < q$.

Llave pública maestra del usuario U es g^x.
Llave privada maestra del usuario U es x.

U:	Selecciona $\gamma \in_R Z^*_q$. Pone $\tilde{a} = g^\gamma$ y $\tilde{b} = \tilde{a}^x$.
$U \rightarrow O$:	Envía $(\tilde{a}, \tilde{b})$.
O:	Selecciona $r \in_R Z^*_q$. Pone $a = \tilde{a}^r$.
$O \rightarrow U$:	Envía a.
U:	Computa $b = a^x$.
$U \leftrightarrow O$:	Ejecutan el protocolo Π para mostrar que $\log_a b = \log_{\tilde{a}} \tilde{b}$.
U, O:	Recuerdan el nym de usuario $N = (a, b)$.

Nota: En el caso especial de que O sea una AC, el usuario debe enviar (g, g^x) en lugar de $(\tilde{a}, \tilde{b})$.

Fig. 2. Generación del nym.

y que ya se cuenta en la implementación. Por lo tanto, esto da garantía de efectividad en la autenticación del nym e integridad del mismo, ya que no está en juego, porque sólo se transmite el resultado.

El nym también puede tomarse como llave pública para firmas y cifrado, sin embargo, aquí no se recomienda esa alternativa por cuestiones de seguridad del mismo, la finalidad se recomienda hacerse con otro par de llaves.

El protocolo de generación de seudónimos forma parte del protocolo del registro en el que el usuario otorga a la organización sus datos generales, quien es la encargada y responsable de ligarlos al nym que se ha generado.

Emisión de credencial

El siguiente subsistema es otro protocolo que permite la emisión de la credencial del usuario seudónimo correspondiente, complementando de esta manera la identidad seudónima de un usuario. Tal protocolo de este subsistema se constituye de dos pasos, los cuales a continuación se mencionan:

1) Emisión de credencial.
2) Transferencia de la credencial obtenida a otra organización.

Las descripciones de los correspondientes pasos se muestran inmediatamente.

Emisión de Credencial

Nym del usuario U con la organización O:
(a, b) donde $b = a^x$.
Llave credencial pública de la organización O:
(g, h_1, h_2) donde $h_1 = g^{s_1}$, $h_2 = g^{s_2}$.
Llave credencial privada de la organización O:
(s_1, s_2).

$O \rightarrow U$: Envía $(A = b^{s_2}, B = (ab^{s_2})^{s_1})$.
U: Selecciona $\gamma \in_R Z_q^*$.
$O \leftrightarrow U$: Corren Γ para mostrar que $\log_b A = \log_g h_2$ con Verificador de entrada γ. Obtienen T_1.
$O \leftrightarrow U$: Corren Γ para mostrar que $\log_{(aA)} B = \log_g h_1$ con Verificador de entrada γ. Obtienen T_2.
U: Recuerda la credencial $C_{U,O} = (a^\gamma, b^\gamma, A^\gamma, B^\gamma, T_1, T_2)$.

Fig. 3. Emisión de credencial.

Emisión de credencial

En la figura 3 se puede observar la continuación del protocolo de interacción que hay entre el usuario y la organización para generar la credencial correspondiente. Aquí O cuenta con su llave credencial secreta que es (s_1, s_2). También O cuenta con su llave credencial pública que es (g, h_1, h_2), donde

$$h_1 = g^{s_1} \quad (8)$$
$$h_2 = g^{s_2} \quad (9)$$

Ahora O calcula b^{s_2} que es A y $(ab^{s_2})^{s_1}$ que es B, para enviárselo a U. U selecciona un número γ del grupo de enteros Z_q^*. Enseguida se lleva a cabo la ejecución del protocolo Γ, dos veces, como se aprecia en la figura. En ambas ejecuciones se pretende primero mostrar la confirmación de las igualdades y, si es así, esto nos indica a primera instancia que el proceso se a llevado sin problemas de inseguridad y por tanto la obtención de T_1 y T_2 respectivamente. Finalmente el usuario obtiene, si se cumple con lo anterior, la credencial correspondiente, que es formada de los siguientes valores a^γ, b^γ, A^γ, B^γ, T_1, T_2.

En general, no hay que olvidar que se puede reforzar la seguridad de estas salidas (nym y credencial), ya sea para almacenamiento o transmisión, con herramientas como: funciones *hash*, esquemas de cifrado de clave pública.

Transferencia de la Credencial a Otra Organización

Llave credencial pública de la organización O:
(g, h_1, h_2) donde $h_1 = g^{s_1}$, $h_2 = g^{s_2}$.
Nym del usuario con organización O':
$(\alpha, \tilde{b})$ donde $\tilde{b} = \alpha^x$.
Credencial de usuario de la organización O:
$C_{U,O} = (a', b', A', B', T_1, T_2)$.

O': Verifica exactitud de T_1 y T_2 como transcripciones para Π_{NI} para mostrar que $\log_{b'A'} = \log_g h_2$ y $\log_{(a'A')} B' = \log_g h_1$.
$U \leftrightarrow O'$: Ejecutan el protocolo Π para mostrar $\log_\alpha \tilde{b} = \log_{a'} b'$.

Fig. 4. Transferencia de la credencial.

Transferencia de la credencial a otra organización

En la figura 4 se aprecia cómo un usuario, con su primer nym y credencial, interactúa con una segunda organización (O'). El usuario le proporciona los siguientes datos para buscar que ésta le otorgue un segundo nym: llave credencial pública de la organización O (g, h_1, h_2) donde $h_1 = g^{s_1}$, $h_2 = g^{s_2}$, credencial del usuario con organización O $(C_{U,O})$ y $(\tilde{a}, \tilde{b})$. Posteriormente la organización O' verifica T_1 y T_2, es decir, confirma las igualdades correspondientes. Finalmente, ambos verifican con el protocolo Π las variables $(\tilde{a}, \tilde{b})$. Si las verificaciones, tanto de validación de la credencial y validación de variables es correcta, la O' le otorga un segundo nym al usuario, que sería $(\tilde{a}, \tilde{b})$.

Lo último nos limita a que la credencial obtenida sólo nos sirva para una segunda organización nada más. Ante esta evidencia se plantea una modificación, que es el de no otorgar como segundo nym a las variables $(\tilde{a}, \tilde{b})$ y nada más utilizarlas como una validación más del proceso. Para poder interactuar con múltiples organizaciones se sugiere que en cada una existan las implementaciones hechas y se calcule un nym y credencial, con el detalle de que a partir de la segunda no haya registro de datos personales.

4.2 Resultados y discusión

No hay que olvidar que el sistema generador de identidades seudónimas ha sido desarrollado en el programa MatLab™ versión 6.5 [5, 6]. A continuación se muestra un ejemplo demostrativo que representa el logro alcanzado a través de la implementación del generador. Para casos prácticos se necesita tener presente que los valores de entrada deben ser grandes.

Ejemplo

Entradas para la *generación del nym*: $p = 59$, $q = 53$, $g = 5$, $x = 2$, $s_1 = 3$, $s_2 = 1$, $\gamma = 3$, $r = 2$.

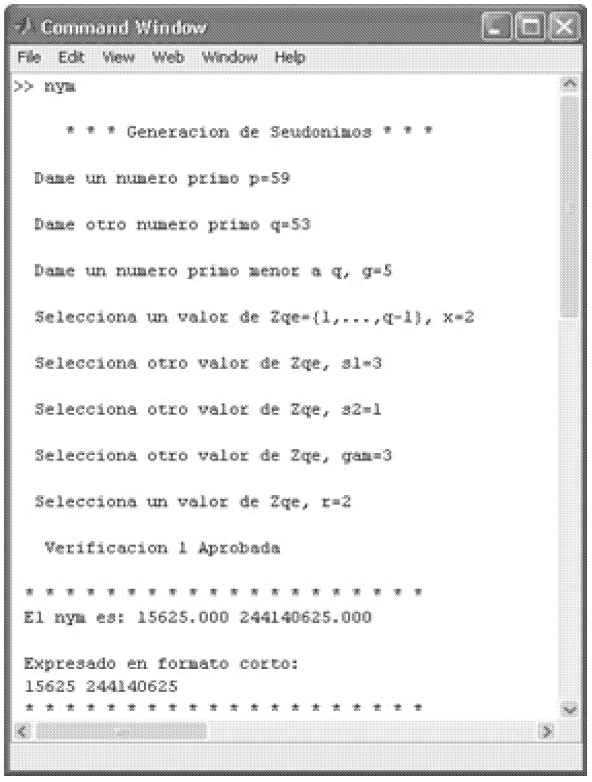

Fig. 5. Nym generado.

En la figura 5, se observa que al ir incrementándose los valores de entrada, el nym correspondiente va de igual forma (en cuestión de seguridad se vuelve más robusto).

La entrada para la *emisión de la credencial*, es: $\gamma = 2$ (véase figura 6). Nótese que la credencial posee mayor robustez que el nym, por el número de los elementos concatenados que la forman, lo cual es importante porque es la que se emplea al momento de interactuar con otras organizaciones. El valor de la variable debe ser mayor a 1, ya que de lo contrario estaríamos divulgando el nym, lo que se opone a las características del sistema.

Transferencia de la credencial a otra organización. En la simulación de la figura 7 se visualiza el cumplimiento de las igualdades logarítmicas, lo cual confirma las validaciones respectivas. Para cada verificación aparecen los resultados de las igualdades logarítmicas, donde el lado izquierdo de dichas igualdades está representado por las variables: *iz*, *iz*2, *iz*3, mientras que el lado derecho está representado por las variables: *dr*, *dr*2, *dr*3. Se puede observar, de igual forma, que en los valores resultantes se ha tomado en cuenta el aspecto de tipo flotante, sin embargo, cabe aclararse que lo que nos interesa

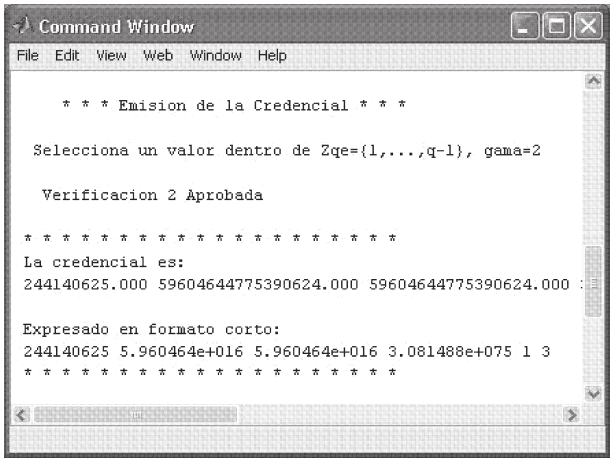

Fig. 6. Emisión de credencial.

son números enteros. En términos generales, los resultados obtenidos en la ejecución del programa coinciden con los cálculos previos (prueba de escritorio).

Por último, se muestran en la tabla 2 los resultados de otros ejemplos adicionales de nym y credencial, con el fin de comparar la variación de tamaño de éstos. Dado que entre mayores sean los números primos de entrada y las combinaciones a partir del grupo, las salidas finales serán mayores (mayor seguridad). Para nym's y credenciales con un mínimo de 30 caracteres es considerado aceptable en cuanto a seguridad se refiere.

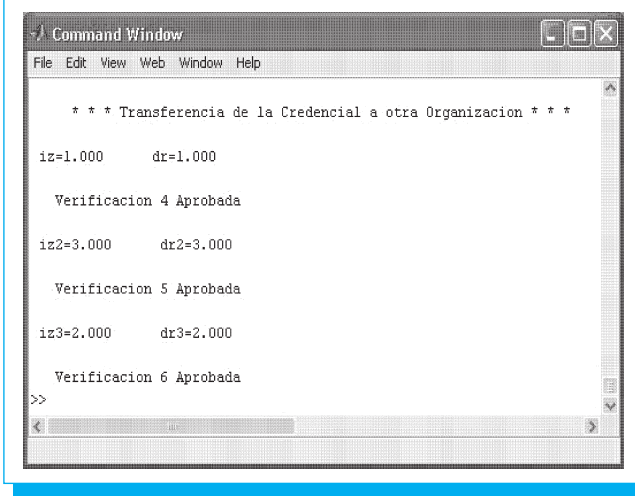

Fig. 7. Simulación de transferencia.

Tabla 2. Ejemplos adicionales de nym y credencial.

NYM S (FORMATO CORTO)	CREDENCIALES (FORMATO CORTO)
1.384129e+010 3.670337e+040	1.384129e+010 3.670337e+040 4.944447e+121 4.683694e+263 3 2
729 2.824295e+011	531441 7.976644e+022 5.075288e+068 7.274974e+148 3.000000e+000 2
6561 2.824295e+011	43046721 7.976644e+022 7.976644e+022 1.179018e+061 1 2
1.628414e+015 2.651731e+030	2.651731e+030 7.031676e+060 2.444756e+243 6.482835e+273 4 1

En general, este sistema de generación de identidades seudónimas puede ser aplicado a diversos ambientes de Internet, buscando proteger la privacidad de la información personal, sin embargo, se puede consultar una aplicación que se le dio como una idea de implantación real en Internet a través de una propuesta teórica de sistema seudónimo [7].

5. Conclusiones

– Se realizó la implementación de un generador de identidades seudónimas (aportación principal), que busca solucionar el problema de falta de privacidad en el manejo de datos personales vía Internet.
– Se establece una innovación en el paso de transferencia de la credencial, con la finalidad de ofrecer la ventaja de interacción con más organizaciones.
– Ofrece autenticación sólida del seudónimo y credencial, así como integridad del proceso.
– La implementación del sistema generador pretende mejorar la confianza en las transacciones comerciales vía Internet, sin embargo, no sólo puede ser utilizado para este caso, sino para cualquier actividad donde la identidad personal se requiera proteger.
– Promueve responsabilidad en el uso de la identidad seudónima, evitando así posibles ilícitos (control de conocimiento de datos personales).
– Es compatible con otras herramientas de seguridad, lo que permite reforzar: autenticación, integridad y confidencialidad.
– En México, una alternativa como ésta, cobra más relevancia por el simple hecho de un atraso tecnológico y porque ya están sucediendo casos como el mencionado en este artículo.
– Para ser eficaz, un mecanismo seudónimo debe involucrar protecciones técnicas y legales.
– La protección de la privacidad requiere que cada individuo tenga el poder de decidir cómo quiere él que sus datos sean reunidos y usados, cómo son modificados y hasta qué punto éstos pueden ser unidos.
– Anonimidad por completo, conlleva a fraude.
– Seudonimidad, plataforma confiable.

6. Referencias

[1] D. Chaum, «*Security without identification: transaction systems to make Big Brother obsolete*», Communications of the ACM, 28 (10), 1985.
[2] O. Aguayo, «Peligra tu identidad navega en Internet», Periódico *Reforma* (México) sección interfase 5, Febrero 2007.
[3] A. Lysyanskaya, R. L. Rivest and A. Sahai, *Pseudonym Systems, Manuscript*, Revision in submission, 1999.
[4] A. Fúster, D. de la Guía, L. Hernández, F. Montoya and J. Muños, *Técnicas Criptográficas de Protección de Datos*, Alfaomega Ra-Ma, Impreso en México, pp. 255-258, 2001.
[5] D. M. Etter, *Solución de Problemas de Ingeniería con Matlab*, Pearson Education, 1997.
[6] S. Nakamura, *Análisis Numérico y Visualización Gráfica con MATLAB*, Ed. Prentice Hall Hispanoamericana, 1996.
[7] B. H. Nava, *Generador de Seudónimos y Credenciales para Transacciones en Internet*, tesis de maestría, IPN, México, pp. 337, 2007.
[8] R. D. Stinson, *Cryptography: Theory and Practice*, Chapman & Hall/CRC, Whashinton D.C., Third Edition, pp. 171-173, 1996.

Científica: **The Mexican Journal of Electromechanical Engineering**

La revista *Científica* ESIME es una publicación trimestral editada por la Escuela Superior de Ingeniería Mecánica y Eléctrica (ESIME) del Instituto Politécnico Nacional (I PN), que presenta trabajos de investigación o propuestas originales en el área de la Ingeniería Electromecánica y sus ciencias afines.

Los artículos se reciben en la Coordinación Editorial de manera personal con una copia del archivo digital del trabajo y una copia impresa en el Edificio 1, Planta Baja, Dirección de la ESIME Zacatenco, UP A LM, Col. Lindavista, CP. 07738, México, DF; o por medio de correo electrónico: revistacientifipn@yahoo.com.mx, revistaesimez@ipn.mx. Para aclaraciones se puede comunicar al teléfono 5729 6000 con las extensiones 54518 y 54555.