MATHEMATICAL FOUNDATION OF DIGITAL SIGNATURES

Daniela Bojan and Sidonia Vultur

Abstract.The new services available on the Internet have born the necessity of a permanent digital signature service, which should guaranteed the security of electronic transactions. That means to permit the identification of the sender without meeting him/her and to permit the verification of data integrity. Digital signature is a response to all this needs and it is realized by using cryptographic methods with public keys.

Keywords and phrases: digital signature, cryptographic algorithm, public/private keys, cipher, security.

1.Digital signature vs. handwritten signature

The concept of `public key cryptography` was introduced by Whitfield Diffie and Martin Hellman in 1975. The cryptography based on public key, uses a pair of keys for encryption: a `public key` (which encrypts data) and a `private` or `secret key` (for decryption). A digital signature serves the same purpose as a handwritten signature. It can be seen as a homologous of a handwritten signature, in the computer world. The major difference between those two signatures is that the handwritten is very easy to counterfeit. Digital signature is nearly impossible to counterfeit, plus it enables the recipient of information to verify the authenticity of the information's origin and also verify that the information is intact. It also prevents the sender from claiming that he/she did not send the information [Ivan2002].

The digital signature consists of two phases [Rosca2004]:

- *data signature* - which implies data encipher and generates both with a hash function, a fixed-length data item, known as a message digest. After that, the digest is signed by using the private key of the signer;
- *signature verification* - which is realized by using the public key of the sender. This verification provides authentication and data integrity.

2. The mathematical base of the digital signature

The algorithms used to generate the digital signatures are very slow and they produce an enormous volume of data, in practice. An improvement on the digital signature process is the adition of a `hash function`. The hash function produces a fixed-length output (the digest).

The digital signature process consists of four principals phases [aici imi zice Ani autorul]:

- the creation of a digest using the hash function;
- the encipher of the digest using the private key of the sender, which is signing in this way;
- the document is sent to the recipient;
- the recipient verifies the signature in three steps:
  1. the creation of a new digest (digest of the signed document);
  2. the decipher of the signed digest by using the public key of the sender;
  3. the two digests are compared; if they are similar than the signature is validated.

The cryptographic algorithms that can be used by the implementations of the existing digital signature systems, are:

- for digest: MD2, MD5 (Message Digest), SHA (Secure Hash Algorithm);
- for signature: RSA (created by Rivest-Shamir and Adleman), ElGamal, DSA (Digital Signature Algorithm).

2.1. RSA cryptosystem

This method was proposed in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman and became a standard for many organizations, because it is recognized as being the certain available method for encipher and authentication. The impossibility of big, integer numbers factoring represents

the mathematical substantiation which the RSA system is based on. The functions used for encipher and decipher are exponentials (the exponent represents the key) and the calculations are made in modulo n rests class ring.

- **The systems parameters**
  - **p** and **q** are two very big, prime, secret numbers (a number consists of 100 decimal digits);
  - the **n modulus**, made public, is obtained as the secret product of the two big, prime numbers: $n = p * q$;
  - **Euler's indicators** $\varphi(n) = (p-1) * (q-1)$;
  - **PRIV, the secret key**, chosen as an related integer to $\varphi(n)$ (preferable to be in the interval $[max(p,q)+1, n-1]$);
  - **PUB, the public key**, which is an integer calculated (using Euclid algorithm) as multiplicative reverse modulo $\varphi(n)$:

$$PUB = inv(PRIV, \varphi(n));$$

  - **M, the electronic document**;
  - **H(M), the documents digest**, calculated using a **hash function, H**.

- **The encipher and the signature of the document**

  Unlike DSS or El Gamal systems, which can be used only for digital signature, RSA can be used both for encipher and for signature of the document. Because of encipher and decipher which are mutually inverse functions, RSA can be used for encipher and for authentication. Theoretical base of RSA, *the Fermat theorem generalization* (offered by Euler), enforces the following necessity: PUB and PRIV to be inverse multiplicative modulo $\varphi(n)$, that is:

$$PUB * PRIV = 1 \ mod \ \varphi(n).$$

a) RSA enciphering function - supposing that one person A wants to send a message M, to a second person B. In this case, the first person A creates (using the exponential process) a coded text C (using the public key of the second person). Then, the message is sent to second person, who deciphers the message M. As long as only he knows the public key, he's the only one who can decipher the message [Patriciu1994].

- A person enciphers the message

$$C \ = \ M_B^{PUB} \ mod \ n_B;$$

- B person deciphers the coded message

$$M \ = \ C_B^{PRIV} \ mod \ n_B \ = \ (M_B^{PUB})_B^{PRIV} \ mod \ n_B.$$

b) RSA digital signature function - supposing that one person A person wants to send a message to a person B. (B must be sure that the message has been sent from A). The A person creates a digital signature, using his private key and sends the message M and the signature S to B person. B person verifies the signature, using the exponential process.

- A person signs the digest $(H(M))$

$$S \ = \ (H(M))_A^{PRIV} \ mod \ n_A;$$

- B person verifies the authentication

$$H(M) \ = \ S_A^{PUB} \ mod \ n_A.$$

2.2. EL GAMAL digital signature system

In many cryptographical protocols two parties wish to begin communicating. However, assume they do not initially possess any common secret and thus cannot use secret-key cryptosystems. The key exchange by the Diffie-Hellman protocol remedies this situation by allowing the construction of a common secret key over an insecure communication channel.The cryptographic method elaborated by El Gamal is based on the discreet logarithm problem [Cobb2004]. The El Gamal cryptosystem has been used with success in many applications, although it is more slow in ciphering and authentication than RSA and the signature is bigger than RSA signature.

- **The systems parameters**
  - $PRIV_A$**, the private key**, which is an integer positive number;
  - PUB_A**, the public key**:

$$PUB_A \ = \ a_A^{PRIV} \ (mod \ n),$$

where: a - is a constant known by every person in system and n - is a big prime number;
- **M**, an electronic document which would be signed;
- **H(M)**, the digest calculated using a *hash function* $H, 0 <= H(M) <= n-1$.

- **The signature of a document** - the signature of a document (M) is realized using the following algorithm:
  - the digest $H(m)$ is calculated;
  - a number K between $[0, \ n-1]$ is generated, so that the most big common divider of $(K, \ n-1) = 1$;
  - a number r, $r \ = \ a^k \ (mod \ n)$ is calculated;
  - a value s is calculated using the private key of the emitter:

$$H(M) \ = \ PRIV_A * r + K * s (mod \ (n-1)).$$

The signature of the M document is represented by the pair:

S=(r, s).

- **The verification of the signature** - A user can verify the documents authentication as long as he/she get the document, M and the signature, $S = (r, \ s)$. For that, the user should calculate two values Val1 and Val2 and compare them:

$$Val1 = a^{H(M)} \ mod \ n$$

and

$$Val2 = (PUB_A)^r * r^s \ mod \ n.$$

2.3.DSS digital signature standard

The **DSA - Digital Signature Algorithm** was elaborated by NIST (National Institute of Standards and Technologies) in 1991 and published in 1994. It was adopted as the DSS standard (Digital Signature Standard). The DSS cryptosystem is based on discreet logarithm and is usually used only for authentication [Menesez1996].

- **The systems parameters**:
  Globals parameters (which are the same for everybody):
  - **p** is a prime number, between $(2^{511},\ 2^{512})$;
  - **q** is a prime divider of $(p-1)$, between $(2^{159},\ 2^{160})$;
  - **g** is an integer with the following property:

$$g = h^{(p-1)/q}\ mod\ p,$$

  where h is an prime integer relative to p, between $(0,\ p)$, so that:

$$h^{(p-1)/q}\ mod\ p\ >\ 1;$$

  - **H** is a hash function used to generate the digest of the message.

  Users parameters:
  - $PRIV$, **the private key**, which is an integer between $(0,\ q)$;
  - PUB, **the public key**, an integer calculated so that:

$$PUB\ =\ g^{PRIV}\ mod\ p.$$

  Signatures parameters
  - **M**, the electronic message;
  - **k**, an integer between $(0,\ q)$, different for every signature.

- **The document signature**
  The digital signature S of an electronic document M is a pair $S = (r,\ s)$ and is made using the secret key of emitter user, $PRIV_A$. After choosing an integer k between $(0,\ q)$, prime with q, r is calculated:

$$r = (g^k\ mod\ p)\ mod\ q;$$
$$s = ((k^{-1})\ (H(M) + PRIV_A * r))\ mod\ q.$$

- **The document signature verification**
  After an user B received the electronic document M and the signature $S = (r,\ s)$, he calculates:

$$w = s^{-1}\ mod\ q.$$

  The signature is validated if the following equation is verified:

$$r = r',$$

where r' is calculated like that:

$$r' = (g^{H(M)*w} * (PUB_A)^{r*w} \ mod \ p) \ mod \ q.$$

3. Conclusions

Digital signatures are used to detect unauthorized modifications to data and to authenticate the identity of the signatory. Thus, use of digital signatures usually involves two processes, one performed by the signer and the other by the receiver of the digital signature:
Digital signature creation uses a hash result derived from and unique to both the signed message and a given private key. For the hash result to be secure, there must be only a negligible possibility that the same digital signature could be created by the combination of any other message or private key.
Digital signature verification is the process of checking the digital signature by reference to the original message and a given public key, thereby determining whether the digital signa ture was created for that same message using the private key that corresponds to the referenced public key [Mollin2001].

4. Challenges and Opportunities

The prospect of fully implementing digital signatures in general commerce presents both benefits and costs. The costs consist mainly of: **Institutional overhead**: The cost of establishing and utilizing certification authorities, repositories, and other important services, as well as assuring quality in the performance of their functions.
Subscriber and Relying Party Costs: A digital signer will require software, and will probably have to pay a certification authority some price to issue a certificate. Hardware to secure the subscriber's private key may also be advisable.
On the plus side, the principal advantage to be gained is more reliable authentication of messages. Digital signatures, if properly implemented and utilized offer promising solutions to the problems of: **Impostors**, by minimizing the risk of dealing with imposters or persons who attempt to escape

responsibility by claiming to have been impersonated; **Message integrity**, by minimizing the risk of undetected message tampering and forgery, and of false claims that a message was altered after it was sent; **Formal legal requirements**, by strengthening the view that legal requirements of form, such as writing, signature, and an original document, are satisfied, since digital signatures are functionally on a par with, or superior to paper forms; and

References

[1] Cobb, C. - "*Cryptography for Dummies*", John Wiley and Sons, 2004.

[2] Ivan, I., s.a. - "*Semnatura electronica si securitatea datelor in comertul electronic*", Revista "Informatica Economica", nr.3/2002.

[3] Menesez, A., Van Oorschoot, P., Vanstone, S. - "*Handbook of Applied Cryptography*", CRC Press, 1996.

[4] Mollin, R., A. - "*An Introduction to Cryptography (Discrete Mathematical and Applications)*", CRC Press, 2001.

[5] Patriciu, V. - "*Criptografia si securitatea retelelor de calculatoare*", Ed. Tehnica, Bucuresti, 1994.

[6] Patriciu, V., s.a. - "*Securitatea comertului electronic*", Ed. All Beck, 2001.

[7] Rosca,Gh., s.a. - "*Comertul electronic. Concepte, tehnologii si aplicatii*", Ed. Economica, Bucuresti, 2004.

[8] Vasilache, D. - "*Plati electronice - o introducere*", Ed. Rosetti Educational, Bucuresti, 2004.

Authors:

Daniela Bojan
Department of Finance Science,
University Bogdan Vodă,
Cluj Napoca, Romania.
e-mail:daniela.bojan@ubv.ro

Sidonia Vultur
Department of Computer Science,
University Bogdan Vodă,
Cluj Napoca, Romania.
e-mail:sidonia.vultur@ubv.ro