ISSN 2320 -2610
Volume 6, No.4, July - August 2017
International Journal of Multidisciplinary in Cryptology and Information Security
Available Online at http://www.warse.org/IJMCIS/static/pdf/file/ijmcis01642017.pdf

The Creation of Steganographic Effect in the Systems of Electronic Signature

Teimuraz Sharashenidze
Georgian Technical University, Geogia, teimuraz555@yahoo.com

ABSTRACT

As is known, the method of electronic digital signatures is used to protect the transmitted information from unauthorized changes, in the channels of communication, from the moment of sending the document to reception by the receiver. The task of encryption of the information itself in this method is not worth it. When using this method, in some cases, the task is to hide some of the transmitted information from unauthorized persons who should not guess the existence of such information. The article introduces an algorithm for implementing the "Steganography" effect, when applying the method of electronic digital signatures based on the RSA method. The article describes the corresponding algorithm, gives a practical example of the implementation of this algorithm. A conclusion is drawn. That the application of this algorithm does not require a change in the RSA method, do not introduce new requirements, but allows you to close a portion of the transmitted information to unauthorized persons.

Key words: public key, hash-function, secret key, “steganographic” effect, digital signature, asymmetric encoding, RSA.

1. ALGORITM CREATION

It is known [1, 2] that “electronic signature” (also often called “electronic digital signature”) is a requisite of an electronic document that is created by cryptographic transformation of document by means of signer’s secret key. It confirms that document hasn’t been modified, i.e. it hasn’t been changed from the moment of creation to the moment of reception. Also sender is identified.

“Electronic Signature” guarantees:

1. Control of integrity of transferrable data;
2. Protection of transferrable data from distortion;
3. Responsibility of sender;
4. Explicit determination of document’s author.

All these components are included in legislation of many countries.

It is known that asymmetric cryptographic systems, compared to symmetric, require more time to encode and decode data. Therefore, they aren’t used for encoding large text files, but if we consider technology of secret key distribution (exchange), then they have obvious advantage over symmetric systems.

So symmetric technique of encoding is mainly used for development of software modules of “electronic digital signature”, when it is not necessary to encode large chunks of data. However, in this case concealment of data (non-sanctioned access) is not possible in any form.

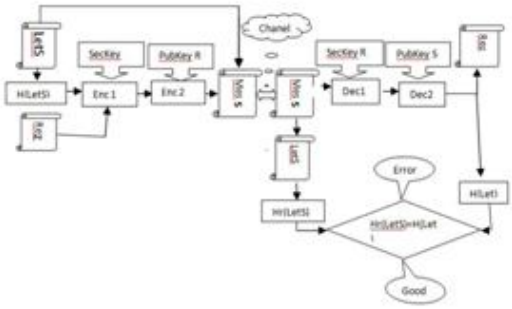

Figure 1: Block diagram

Figure 1 shows modified algorithm with so-called “steganographic” effect. It is based on classic algorithm of “electronic signature” with technique of asymmetric encoding. Modified algorithm takes into account preliminary exchange of “public keys” Public R and Public S between sender and recipient.

Sender party sends short, secret, hidden (encoded) textual data in the form of resolution Rez with initial plaintext Let S. It should be invisible for user who has non-sanctioned access to the channel. At the initial stage hash-function H (Let S) of plaintext Let S is calculated and then it is encoded with sender’s secret key SecKey S by means of asymmetric technique at the first node Enc 1. The resulted encoded information is once again encoded with recipient’s public key Public R at the second node Enc 2 with the same technique of encoding. Encoded data and plaintext Let S gives final data Mes S that includes plaintext and encoded data (H(Let S) + Rez). The final data is sent to recipient in the channel.

The inverse happens at the recipient’s side. Recipient takes out plaintext, calculating its hash-function Hr (Let S), as well as accompanying encoded data (H(Let S) + Rez). In parallel, this data gets to the first node Dec 1 of decoding, where data is decoded with recipient’s secret key SecKey R. Afterwards, at the second node Dec 2 of decoding, sender’s public key PubKey S is used for decoding. Decoded information is divided into resolution Rez and sent hash-function H (Let S). The result H (Let S) and calculated hash Hr (Let S) are compared and if they are equal, then the received data is checked for integrity and correctness.

The innovation of offered algorithm is that it is impossible to read hidden resolution. Only plaintext is readable that may not contain the sensitive information.

2. PRACTICAL EXAMPLE

For instance, let us consider the case when the plaintext is sent.

In the list of executed operations we have:

- send data to client A;
- transfer money to client B;
- prepare visit in city C.

The plaintext also contains hidden resolution "Only p.3 Giorgi". We offer realization of algorithm [3] that is created on the basis of algorithm RSA of asymmetric encoding. We have the following secret and private keys for the sender:
ps=29,qs=46874467,es=4153,ds=316033,ns=1359359543
and for the recipient:
pr=113,qr=10528093811,er=19,dr=62060342459,
nr=1189674600643
then the encoded data has the following form if we use classic algorithm of electronic signature (without resolution):
[642406964506, 642406964506, 642406964506, 642406964506, 642406964506, 642406964506, 642406964506, 642406964506, 642406964506, 7551466069, 1075500976813, 51617533504, 844447594438, 338506368779, 1075500976813, 653514397603, 844447594438, 384633090760, 816012050820, 844447594438, 384633090760, 1073348847375, 954514316738, 462706929068, 242523779427, 954514316738, 1073348847375, 462706929068, 844447594438, 462706929068, 105875748524, 384633090760, 242523779427, 642406964506, 642406964506, 642406964506, 642406964506, 692444876697, 1189107212743, 153499250132, 323407696778, 1189107212743, 184309758866, 462706929068, 7551466069, 927253312372, 323407696778, 814291523765, 193679945694, 614256348667, 431811248149, 1073348847375, 343177252365, 51617533504, 653514397603, 47319043241, 967770689814, 51617533504, 904060357479, 653514397603, 275274386322, 692444876697, 369241508768, 57607641754, 201583710840, 105875748524, 992064852680, 367677351338, 201583710840, 51617533504, 514227014430, 613073268033, 79126173423, 93709986889, 100609357749, 653514397603, 678170375144, 1156582046178, 1067232726409, 184309758866, 184309758866, 692444876697, 495350561827, 967770689814, 559032041625, 751389949180, 285234204072, 338506368779, 206528413020, 153499250132, 967770689814, 79126173423, 559809916314, 1099410716939, 967770689814, 927253312372, 653514397603, 213739731802, 275274386322, 692444876697, 653514397603, 1073348847375, 285234204072, 613073268033, 79126173423, 992064852680, 992064852680, 57607641754, 751389949180, 255277346433, 514227014430, 79126173423, 816012050820, 153499250132, 343177252365, 93709986889, 191536923318, 298855825611, 551818874415, 514227014430, 323407696778, 1189107212743, 323407696778, 1105264422850, 1105264422850, 642406964506, 642406964506, 642406964506, 642406964506]

but in the case of resolution we have:
642406964506, 642406964506, 642406964506, 642406964506, 596792189097, 906303964178, 602737566139, 1184740141569, 525035202624, 727953623319, 1137208572348, 300483695515, 525035202624, 51967864004, 727953623319, 832401576256, 1117191517564, 60184090704, 525035202624, 1039886707898, 844447594438, 341509514910, 1149188756762, 602737566139, 60184090704, 602737566139, 1014052432991, 844447594438, 1014674791496, 1054682163345, 1073348847375, 844447594438, 1137208572348, 319210170733, 604242702353, 602737566139, 832401576256, 319210170733, 604242702353, 575416516257, 642406964506, 642406964506, 642406964506, 642406964506, 7551466069, 1075500976813, 51617533504, 844447594438, 338506368779, 1075500976813, 653514397603, 844447594438, 384633090760, 816012050820, 844447594438, 384633090760, 1073348847375, 954514316738, 462706929068, 692444876697, 954514316738, 992064852680, 242523779427, 844447594438, 462706929068, 105875748524, 384633090760, 242523779427, 642406964506, 642406964506, 642406964506, 642406964506, 692444876697, 1189107212743, 153499250132, 323407696778, 1189107212743, 184309758866, 462706929068, 7551466069, 927253312372, 323407696778, 814291523765, 193679945694, 614256348667, 431811248149, 1073348847375, 343177252365, 51617533504, 653514397603, 47319043241, 967770689814, 51617533504, 904060357479, 653514397603, 275274386322, 692444876697, 369241508768, 57607641754, 201583710840, 105875748524, 992064852680, 367677351338, 201583710840, 51617533504, 514227014430, 613073268033, 79126173423, 93709986889, 100609357749, 653514397603, 678170375144, 1156582046178, 1067232726409, 184309758866, 184309758866, 692444876697, 495350561827, 967770689814, 559032041625, 751389949180, 285234204072, 338506368779, 206528413020, 153499250132, 967770689814, 79126173423, 559809916314, 1099410716939, 967770689814, 927253312372, 653514397603, 213739731802, 275274386322, 692444876697, 653514397603, 1073348847375, 285234204072, 613073268033, 79126173423, 992064852680, 992064852680, 57607641754, 751389949180, 255277346433, 514227014430, 79126173423, 816012050820, 153499250132, 343177252365, 93709986889, 191536923318, 298855825611, 551818874415, 514227014430, 323407696778, 1189107212743, 323407696778, 1105264422850, 1105264422850, 642406964506, 642406964506, 642406964506, 642406964506]

The result doesn't contain any public data (quantity of encoded blocks) that will help non-authorized person perceive or understand text of resolution. In this case cryptographic reliability depends only on the length of encoding key. In our example, if we have resolution, time of encoding is tr=0.6864008903503418s, and without resolution-t=0.6552009582519531s.The difference tr-t= 0.031199932098388672s is so insignificant that we can conclude: realization of offered algorithm doesn't have practical impact on time of algorithm operation. In the case of necessity, we can modify the software and mitigate even such small quantitative differences of encoded blocks.

3. CONCLUSIONS

We can conclude that offered algorithm strengthens the confidentiality of data, gives "steganographic" effect without modification of the basic algorithm of electronic signature, doesn't introduce requirement of creation of new parameters and practically doesn't deteriorate time specifications.

REFERENCES

1. Arto Salomaa. **Public-Key Cryptography .** Springer-VerlagBerlin Heidelberg New York LondonParis Tokyo Hong Kong Barcelona
2. Andrew Tanenbaum, David Wetherall. **Computer Networks**. Upper Saddle River,New Jersey 07458
3. Teimuraz Sharashenidze, **System "Bastioni"**. Certificate of authorship.GEORGIA #4904 .2011