Analyzing the use of combined cryptography for increasing the security of information

Florim Idrizi, Ilia Ninka

Abstract— Data security means protecting data from misuse, and controlling that access to this data. In this way, data security helps us for maintaining privacy and securing personal data. Privacy represents secrecy of data, meaning that only authorized people can access them. In this article we will explain some concepts of combined cryptography in order to increase the security of the information that is sent electronically. Further, we will conduct some experiments with combined algorithms AES-RSA, DES-RSA, Blowfish-DSA by using the LabWIEW software. Furthermore, we will measure the speed of some combined algorithms in terms of the number of the characters that are encrypted/decrypted. Form our analysis we point out that the speed of combined algorithms is not very low, taking into account the security of data transmitted electronically.

Index Terms— AES, DES, Blowfish, DSA, encryption, decryption, LabView

1 Introduction

The concept of secure messages in terms of cryptography has been used since the ages of Roman Empire. It is thought that Julius Cesar has been one of the first to create the cryptographic system for sending secret military messages to his generals. During the history, one problem has limited the overall usage of cryptography. This problem is the key management. In the cryptographic systems, the term key is referred to a numerical value that is used from an algorithm to change the information, in order to make this information secure and visible only for individuals that posses the adequate key to reveal that information. Consequently, key management has to do with the secure key administration in order to make available this key in the right time for the right people.

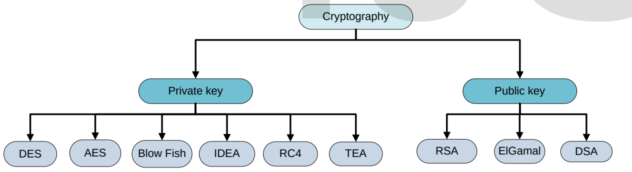


Fig. 1. .Algorithms with public and secret key

The importance of cryptography is immense due to the massive usage of the Internet, ehere we deal with:

- Sensitive data transmission
- Distance access to various information systems
- Information that are been used through electronic business, such as: e-commerce, m-commerce, e-banking, e-government, etc.

Applying cryptography in Internet imposes the need for employing several security components

- Authentication. The process of identification of participants in the communication process.
- Privacy/Confidentiality. This means to eliminate the possibilities of reading accessing messages by foreigners.
- Integrity. To eliminate the possibility of changing the messages that are being sent, so that the receiver to have the original information sent.
- Non-repudiation. The receiver must be completely sure that the information is sent by the receiver, meaning that this information has not been sent by another person.

Cryptography not only protects data from unauthorized access, but it also covers the process of the data user identification.

Data security is an essential part of an organization; it can be achieved by the usinë various methods. In order to maintain and upgrade the model still efforts are required and increase the marginally overheads. The encrypted data is safe for some time but never think it is permanently safe. After the time goes on there is chance of hacking the data by the hacker. Fake files are transmitted in the same manner as one can sends the encrypted data. The information about the key is present in the encrypt data which solves the problem of secure transport of keks from the transmitter to receiver [1,2]. In case of practical sistem encrypted data is passed through the various stations which are capable to re-encrypt the data by their own key. At the time the previous keys are discarded, this will make the system more secure. There are many algorithms available in the market for encrypting the data. Encryption is the process in which plaintext has been converted into the encoded format ciphertext with the help of key [3].

2. Combined cryptography

Combining the secret key and public cryptography can result in better results regarding the encryption. In this process, one must take into account the points where one algorithm is weaker than another. Encryption starts by generating secret key. The secret key used is safe and fast. During the public key encryption, a major problem was how to reach the receiver by using secret key. This is enabled by public key. In this case, the public key of the receiver is used for encrypting only the secret key. Normally, the public key cryptography is slower, nevertheless, the size of the secret key is little and this would not affect the speed limitation of encryption and decryption.

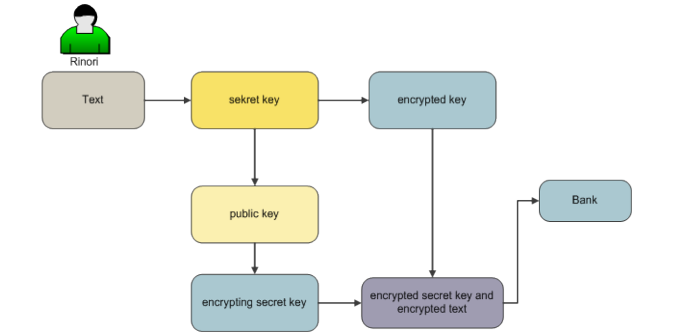


Fig. 2. Combined encryption

The last process is connecting the encrypted secret key with the encrypted text for transferring the message to the receiver. We must emphasize that transferring messages through Internet, unknown individuals cannot read this text because the secret key is encrypted by the secret key of receiver. It is only the sender who can decrypt that with the help of his private key.

The use of public/secret encryption for encrypting the secret key offers reasonable solutions by protecting the secret key from copying it through the transmission process. Also, there is no need for prior deals between peers that participate in the transmission for exchanging the secret key.

Decryption starts with the acceptation of the encrypted secret key and the encrypted text. Afterwards, the encrypted key and the encrypted text are decrypted in this way. After encrypting the secret key of the sender with the public key of the receiver, the encrypted secret key will be decrypted with the receiver secret key, which results with gaining the sender secret key. The sender secret key is used for decrypting the encrypted text where the original text appears.

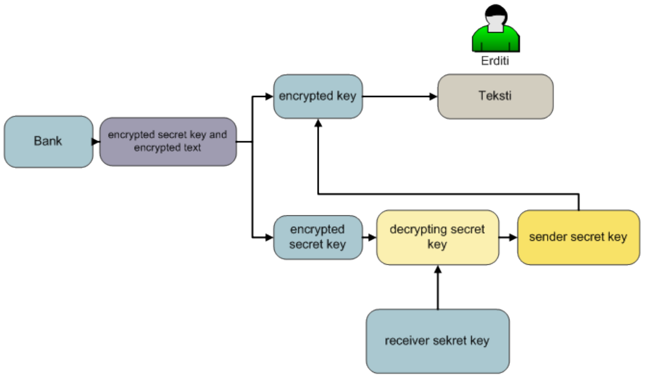


Fig. 3. Combined decryption

The combined cryptography represents the foundation for many modern encryption solutions, such as: e-main encryption, VPN encryption etc.

However, combined cryptography must assure that the encrypted message comes from the sender. It can happen that a third person can make use of the receiver public key and encrypts the secret key used for encrypting the message. The third person can share that on Internet. The receiver initially decrypts the secret key by using his private key and the message by using the secret key of the sender. The receiver has received one unwanted message by an unwanted receiver. To make sure that the message comes from the right sender, we use digital certificates

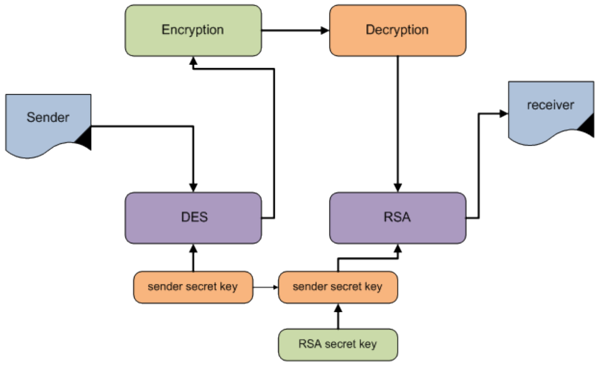
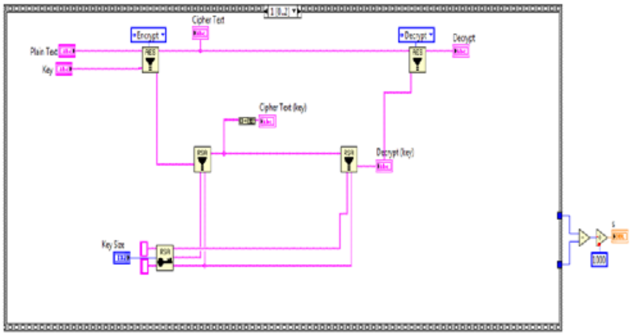
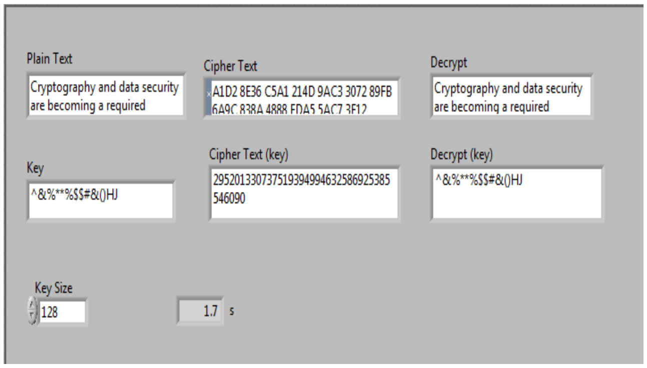


Fig. 4. Combining DES and RSA

3. ANALISYS OF COMBINED CRYPTOGRAPHY AES – RSA BY USING LABVIEW

RSA has two keys, one private and one public. RSA is implemented as a software. With computers it's hard to code plain text and to decode cipher text using RSA. If the key is sent separately encrypted with RSA, then the recipient can use it to decrypt messages encrypted with DES. AES is faster and more secure. For its encoding and decoding is used the same key. If AES is used for communication (encoding of the message), the receiver must have the key, so there appears the problem of key exchange. This problem is solved by using asymmetric algorithms such as RSA. Here the sender sends the message using the private key. Receiver decodes the message with the public key. Anyone can use this public key. So, the receiver can decode the message. Asymmetric algorithms are much slower but the key exchange can be accomplished with asymmetric algorithms and encryption of data with symmetric algorithms. Both are very easy to implement.





Plain Text: Cryptography and data security are becoming a required

Cipher Text: A1D2 8E36 C5A1 214D 9AC3 3072 89FB 6A9C 838A 4888 FDA5 5AC7 3F12

Decrypt: Cryptography and data security are becoming a required

Key: ^&%**%$$#&()HJ

Cipher Text (key): 2952013307375193949946325869253855 46090

Decrypt (key): ^&%**%$$#&()HJ

Key Size: 128

1.7 s

Fig. 5. The realization of AES – RSA algorithm using LabVIEW

TABLE 1

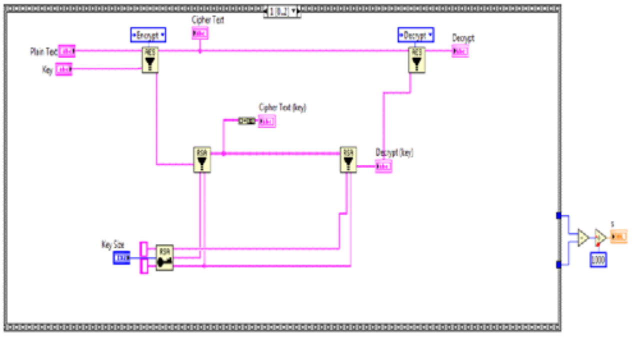
THE SPEED OF AES – RSA IN TERMS OF CHARACTER NUMBER ENCRYPTED AND DECRYPTED

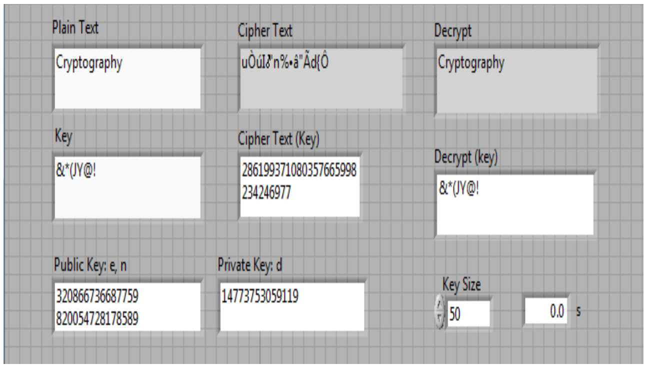
Characters number	1000	2000	3000	4000	5000	10000
Time	1.7s	2.1s	2.6s	3.2s	3.8s	6.4s

From the table we can conclude that by increasing the character number that is being encrypted and decrypted, the time is increased in continuous manned. This means that the algorithm spped depends on the character number.

4 ANALISYS OF COMBINED CRYPTOGRAPHY DES – RSA BY USING LABVIEW

RSA has two keys – one private and one public. RSA is implemented as software. It is hard to code the plaintext and to decode the ciphertext with RSA. DES has the same key for encryption and decryption. DES is implemented in hardware and it is fast. Any communication between two businesses can use different keys, and the key can be exchanged. If the key is sent separately encrypted with RSA, then the receiver can use it for decrypting the encrypted message with DES. DES is faster for generating signature but is slower in encryption. It is faster when decryption and the security can be considered comparable in equivalent way with RSA key with same size[4].





Plain Text: Cryptography

Cipher Text: uÒúÌ8"n%•â"Ãd{Ô

Decrypt: Cryptography

Key: &*(JY@!

Cipher Text (Key): 2861993710803576659982 34246977

Decrypt (key): &*(JY@!

Public Key: e, n: 320866736687759 820054728178589

Private Key: d: 14773753059119

Key Size: 50

0.0 s

Fig. 6. The realization of DES – RSA algorithm using LabVIEW

TABLE 2

THE SPEED OF DES – RSA IN TERMS OF CHARACTER NUMBER ENCRYPTED AND DECRYPTED

Character number	1000	2000	3000	4000	5000	10000
Time	0.2s	0.4s	0.5s	0.6s	0.8s	1.4s

From the table we can conclude that realizacion of combined cryptography by usinë DES-RSA is faster comparing AES-RSA algorithms, where the speed of encryption and decryption was slower.

5. ANALISYS OF COMBINED CRYPTOGRAPHY BLOWFISH – DSA BY USING LABVIEW

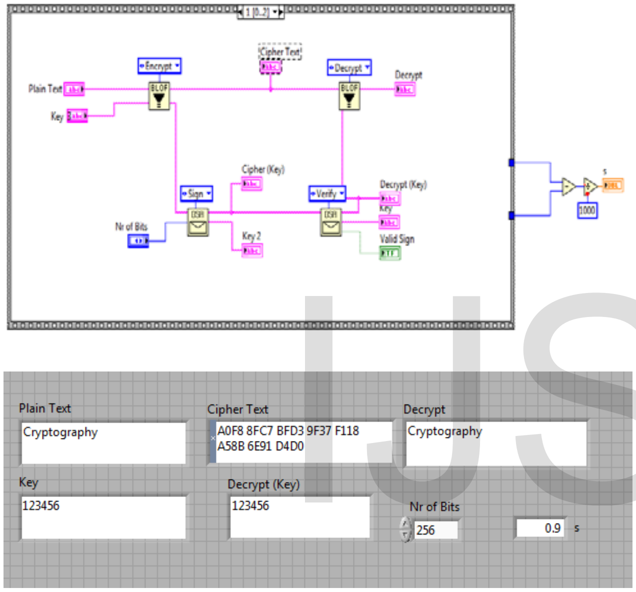
Blowfishis a symmetricblockcipherthatcan be used as a drop-in replacement for Data Encryption Standard or International Data Encryption Algorithm. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for both domestic and exportable use. Blowfish was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms. Since then, it has been analyzed considerably, and is slowly gaining acceptance as a strong encryption algorithm. Blowfish is not patented, is license-free, and is available free for all uses.

As far as I know, this is the first implementation of the Blowfish Algorithm in LabVIEW. With this set of sub-VIs, one can encrypt data in LabVIEW without the need for external software. This can be used to send data securely over Data Socket as well as TCP and UDP communications. It can also be used to protect remote control systems from unauthorized access by encrypting the control communications.

I have added compatibility for the basic blowfish functions with other implantations, and fixed a couple of bugs. The "LabVIEW Blowfish Encryption.vi" uses header info to return an encrypted message back to its original length; because of this, it will likely not be directly compatible with other encryption software even though the software may use the same blowfish encryption method. Without knowing what other software uses for header info, I just used what was convenient for me in LabVIEW [5].

Using DSA with SHA-256 in DNSSEC has some advantages and disadvantages relative to using RSA with SHA-256 when using 2048-bit keys. DSA signatures are much shorter than RSA signatures; at this size, the difference is 512 bits verus 2048 bits. On typical platforms using 2048-bit keys, signing DSA is about three times faster than for RSA, but verifying RSA signatures is more than ten times faster than for DSA.

The cryptographic strength of DSA is generally considered to be equivalent to RSA when the DSA public key and the RSA public keys are the same size. Such an assessment could, of course, change in the future if new attacks that work better with one or the other algorithms are found[6].



Plain Text: Cryptography

Cipher Text: A0F8 8FC7 BFD3 9F37 F118 A58B 6E91 D4D0

Decrypt: Cryptography

Key: 123456

Decrypt (Key): 123456

Nr of Bits: 256

0.9 s

Fig. 7. The realization of Blowfish-DSA algorithm using LabVIEW

TABLE 3

THE SPEED OF BLOWFISH – DSA IN TERMS OF CHARACTER NUMBER ENCRYPTED AND DECRYPTED

Character number	**1000**	**2000**	**3000**	**4000**	**5000**	**10000**
Time	1.0s	1.1s	1.1s	1.1s	1.1s	1.2s

From the table we can conclude that by increasing the character number that is encrypted and decrypted, the time is not increased in continuous manner. This means that the speed of algorithm doesn't depend on the character number but on key size.

6 CONCLUSION

Combined cryptography is widely used when we want to send messages in secure way to the receiver. In this article we explained the concepts of combined cryptography, emphasizing the role of increased security for messages sent over Internet. Further, we have conducted some experiments with combined algorithms AES-RSA, DES-RSA, Blowfish-DSA, by using the LabVIEW software. Furthermore, we measured the speed of some combined algorithms in terms of the number of the characters that are encrypted/decrypted. Form our analysis we pointed out that the speed of combined algorithms is not very low, taking into account the security of data transmitted electronically.

REFERENCES

[1] Ajay Kakkar, Dr. M. L. Singh, Dr. P. K. Bansal, "Efficient Key Mechanisms in Multinode Network for Secured Data Transmission", International Journal of Engineering Science and Technology, Vol. 2, Issue 5, 2010, pp.787-795

[2] Davis, R, "The data encryption standard in perspective", Communications Society Magazine, IEEE, 2003, pp. 5 – 9.

[3] Ajay Kakkar, M. L. Singh, P.K. Bansal, Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication in Multinode Network, International Journal of Engineering and Technology Volume 2 No. 1, January, 2012

[4] "Proposed Federal Information Processing Standard for Digital Signature Standard (DSS)," Federal Register, v. 56, n. 169, 30 Aug 1991, pp. 42980-42982.

[5] http://zone.ni.com/devzone/cda/epd/p/id/3473

[6] http://superuser.com/questions/13164/what-is-better-for-gpg-keys-rsa-or-dsa