MODELING METHODS OF DENYED ENCRYPTION WITH A SHARED KEY

Andrushchak Igor,
Doctor of Technical Sciences, Professor

Androshchuk Igor,
Candidate of Agricultural Sciences, Associate Professor
Lutsk National Technical University

Androshchuk Olena,
Head of the obstetrics-pharmaceutical department
Volyn Medical Institute
Lutsk, Ukraine

Criteria for the construction of deniable encryption algorithms for the implementation of information protection mechanisms such as deceptive traps are proposed, and the developed algorithms of this type are presented. The new implemented requirements are indistinguishability from probabilistic encryption and the identity of the decryption procedure and the use of all bits of the cryptogram for all possible key values. The proposed deniable encryption methods provide high performance and are promising for expanding the arsenal of cryptographic information protection mechanisms used in complex computer security systems.

Keywords: block ciphers, computer security, cryptography, deniable encryption, hash functions, probabilistic encryption, cryptogram.

……..…………………………………………………………………………………..

The concept of deniable encryption (DE) is associated with the problem of ensuring the strength of information encryption in the face of the possibility of so-called duress attacks. These types of attacks imply that the attacker of such resources has an impact on the sender and (or) recipient of messages that force the sender and (or) recipient to reveal the parameters of the encryption process (coercive attack on the message sender) or decryption (coercive attack on the message recipient), for example, the encryption key and random values used in the encryption process.

If it is assumed that the attacker can require both encryption and decryption parameters to be provided, then a two-way coercive attack takes place. Resistance to such attacks is provided by DE algorithms and protocols in that the output ciphertext (cryptogram) can be obtained from various meaningful source messages and (or) various decrypted meaningful texts can be obtained from the cryptogram. The attacker is given encryption parameters that associate the cryptogram with some fictitious meaningful text. The attacker checks that the use of the encryption parameters provided to him actually leads to the conversion of the bogus message into the given cryptogram and (or) to the decryption of the latter into the bogus message. If the check result is positive and the attacker cannot prove the incompleteness of the disclosed text, then the DE algorithm (protocol) is considered secure [1].

In the known literature, the main attention of researchers is directed to DE methods related to public-key cryptoschemes. Such methods are based on the use of open encryption algorithms or public key distribution protocols. It is assumed that the sender and recipient do not have common secret information (shared secret key), and the recovery of a fictitious/real message depends on the random values used.

Interest in DE algorithms and protocols is associated with the prospects for their application in secure distributed computing and secret electronic voting systems. One of the limitations of the practical use of DE procedures is their low performance, which is especially characteristic of public key crypto schemes. The search for new DE algorithms and protocols has led to the development of more efficient DE methods, but practice requires further increase in the speed of crypto algorithms, especially in cases where DE methods are used as a special information protection mechanism in complex computer security tools based on deceptive traps.

Unlike DE schemes based on asymmetric encryption algorithms, DE based on shared key schemes implies the presence of a shared secret (shared secret key) that allows both the sender and the recipient to recover the real message. In this paper, we solve the problem of developing efficient deniable encryption algorithms while providing high resistance to a two-way duress attack based on DE with a shared secret. The combination of performance and durability removes significant restrictions on the practical application of DE algorithms for protecting information in information security tools. At the same time, special requirements are formulated for DE algorithms related to the use of DE to implement protection mechanisms such as deceptive traps. The proposed new requirements are not satisfied by the shared secret DE algorithms known in the literature [2].

The implementation of information protection mechanisms such as deceptive traps is based on the use of DE methods that provide the possibility of sufficiently fast joint encryption of two or more different messages on two or more different keys of a finite length. One of the messages is fictitious and is encrypted with a fictitious secret key, to which controlled access is organized by the intruder.

When decrypting a properly composed fictitious message, the offender is misled (misinformed). However, it should be assumed that the adversary knows the decryption algorithm used by the authorized user and can analyze the cryptogram and its application when performing the decryption procedure against the dummy key. This should not give him reasonable suspicions that, in addition to the fictitious key he received, there is also another key that decrypts the cryptogram into another meaningful message (fig.1)

In other words, the DE algorithm must have properties that will not allow an attacker to distinguish DE from probabilistic encryption based on the cryptogram, the dummy message, and the dummy key.

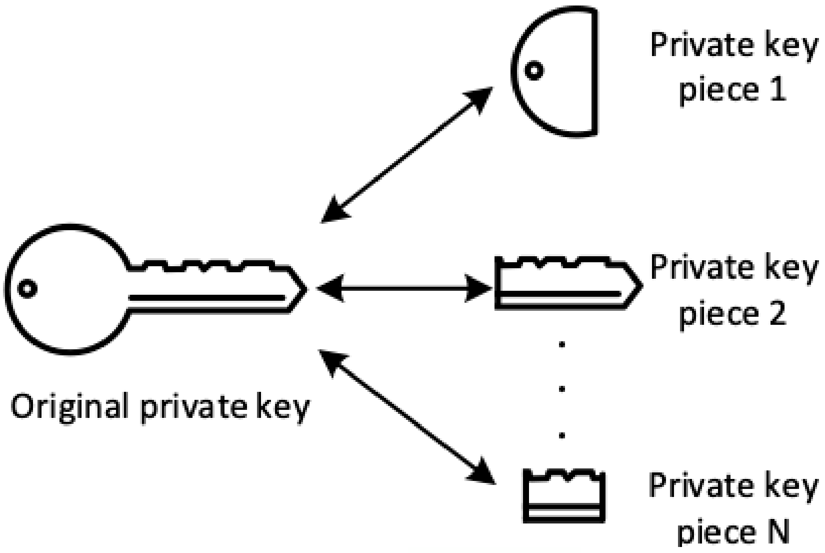

Figure.1 – Key Shards

This defines the following requirements for DE algorithms:

1) indistinguishability by cryptogram from probabilistic encryption;

2) the same decryption procedures for the various keys used;

3) equality (identity of use) of all bits of the cryptogram for all possible values of the decryption key.

These requirements are superimposed on the requirement to use keys of a finite size and provide a sufficiently high performance [3].

They are actually a continuation of the Kerchkoff principle formulated for symmetric encryption algorithms: the cipher must be strong, provided that all the details of the encryption procedure are known to the attacker. For DE algorithms, it is reasonable to supplement this principle with the requirements of computational indistinguishability from a probabilistic encryption algorithm with a known decryption procedure and a known cryptogram.

The meaning of this extension of the Kerchkoff principle is that the attacker cannot reasonably assert (suspect) that the cryptogram contains some other message than the message received using the decryption key he has. Of the three requirements for DE algorithms formulated earlier, the second and third are auxiliary. However, non-compliance with these requirements serves as a source of assumptions that, in addition to a fictitious message, the cryptogram contains other information. The formulated requirements are met if it is possible to specify a probabilistic encryption algorithm that converts a fictitious message using a fictitious key into a cryptogram obtained using the DE algorithm. In this case, the decryption algorithm is specified by some mathematical formula, in which the cryptogram and the decryption key are included as transformation parameters (fig.2).

The DE method based on the use of hash functions or block transformations and described in the section "Deniable encryption method using block transformations" satisfies the three requirements for DE algorithms stated in the "Requirements for shared secret deniable encryption algorithms" section. This is directly evident from the description of the algorithms implemented on the basis of this method.

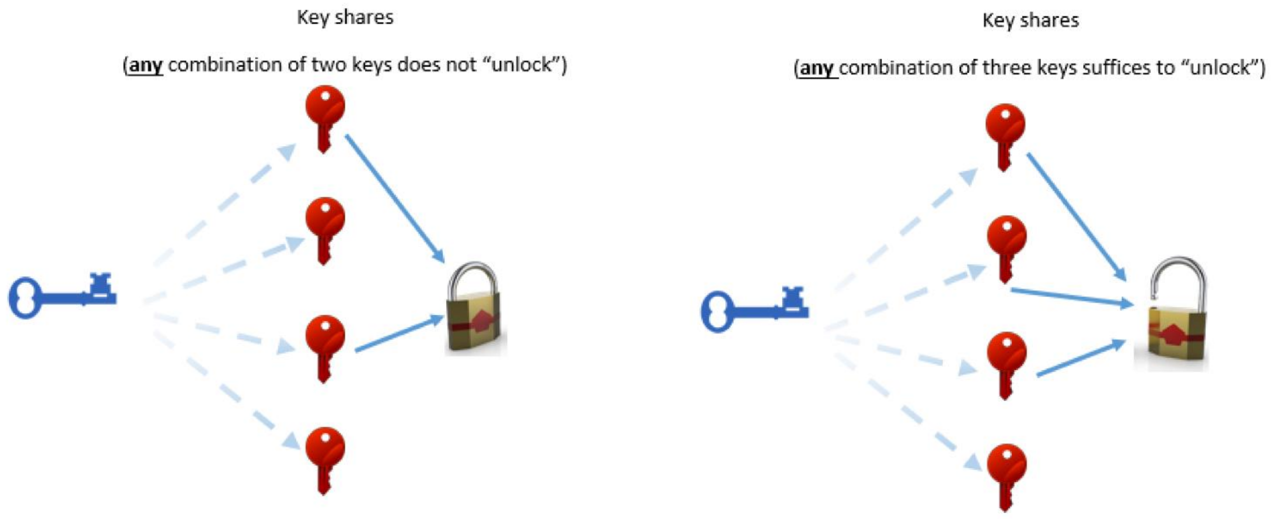
Key shares
(any combination of two keys does not “unlock”)
Key shares
(any combination of three keys suffices to “unlock”)

Figure.2 – Secret sharing: “Splitting” the key into several shares

The DE algorithms described in the previous section clearly satisfy the second and third requirements. Let us show that they also satisfy the requirement of being indistinguishable from probabilistic encryption. To do this, we specify a probabilistic encryption algorithm that, using a fictitious key, converts a fictitious message into a cryptogram. This algorithm will be called the associated probabilistic encryption algorithm [4].

Next, we consider the use of DE algorithms with a shared secret key as an information protection mechanism and formulate requirements for algorithms of this type, focused on use in protection mechanisms that allow the implementation of deceptive traps. This information protection mechanism is new for use in complex information and computer security systems. The developed methods and specific DE algorithms that meet the stated requirements are described. One of the formulated requirements is the indistinguishability of the cryptogram obtained using the DE procedure from the cryptogram obtained using the probabilistic encryption procedure.

The compliance of the developed algorithms with this requirement is justified by indicating the associated probabilistic cipher, for which the decryption procedure coincides with the procedure for decrypting a fictitious message using a fictitious key. The given associated probabilistic ciphers are interesting in that in the process of decrypting the cryptogram, the random values used in the encryption procedure are not uniquely restored, while for the known probabilistic block ciphers, the used random values are uniquely restored in the decryption process. This determines an independent interest in the considered probabilistic encryption algorithms. Also, an independent research task is the development of sufficiently fast DE algorithms with commutative properties [5].

Our preliminary results testify in favor of the possibility of solving the latter problem using the cryptogram generation mechanism based on the solution of the system of comparisons proposed in this paper. The considered algorithms refer to the case of simultaneous encryption of two messages, but they are easily extended to the case of simultaneous encryption of three or more messages.

References:

1. Bo Meng. A Secure Internet Voting Protocol Based on Noninteractive Deniable Authentication Protocol and Proof Protocol that Two Ciphertexts are Encryption of the Same Plaintext // J. of Networks. 2009. Vol. 4. N 5. P. 370–377.
2. Berezin A.N. Method of deniable encryption / A.N. Berezin, A.R. Birichevsky, N.A. Moldovyan, A.V. Ryzhkov // Issues of information security. 2013. No 2, pp. 18–21.
3. Ibrahim M. H. A Method for Obtaining Deniable Public-Key Encryption // Intern. J. of Network security. 2009 Vol. 8. No. 1. P. 1-9.
4. Martseniuk V. Competency-based chellenges of applied artificial intelligence: project FAAI. / V.Marcenyuk, G.Dimitrov, D. Rancic, I.Luptakova, S. Tomovic, M.Bernas, A. Klos-Witkowska, T.Gancarczyk, A.Sverstiuk, I.Andrushchak // Abstaracts of XXXVII International conference Problems of decision making under uncertainties «PDMU-2022». – Sheki-Lankaran, Azerbaijan, 23-25 November 2022. – P. 79-80.
5. Moldovyan A. A., Moldovyan N. A., Guts N. D., Izotov B. V. Cryptography: high-speed ciphers. - St. Petersburg: BHV-Petersburg, 2002. - 495 p.