**REPORTS OF THE NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN**
ISSN 2224-5227
Volume 2, Number 318 (2018), 17 – 22

UDC 004.056.5

A.A. Zhatkanbayev

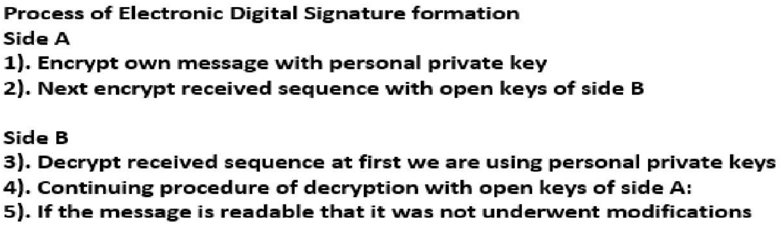
Al-Farabi Kazakh National University, Almaty, the Republic of Kazakhstan
wildlife.kz@gmail.com

EFFECTIVE SCHEME OF STEGANOGRAPHY INFORMATION PROTECTION AND AUTHENTICATION BASED ON MAXIMUM FLOW ALGORITHMS

Abstract. Developed effective scheme of electronic digital signature based on El-Gamal algorithm, transport network and it's blocking flows (output data) produced by Ford Fulkerson maximum flow algorithm serves as additional data for sides authentication. Scheme with the addition of transport networks and it's blocking flows is considered as effective since there exist various sets of identical blocking flows and various transport networks associated with following flows.

Key words. steganography, Ford Fulkerson algorithm, blocking flow, cryptography, flow, authentication.

ElGamal digital signature. ElGamal scheme was created by Taher Elgamal in 1985 [1]. Following scheme is based on public key cryptography, the complexity of calculation discrete logarithm [2]. Developed scheme of steganography based on information concealing within the framework of master degree project can be also applied at the process of authentication. The adjacency matrix of the graph (transport network), including its weights and selectable blocking flows as well as maximum flow is input criteria on which process of user authentication would occur. In parallel for binding these input data to particular user, it is necessary to use tools of Electronic Digital Signature. The process of signing input parameters data would be done in the following manner.



Process of Electronic Digital Signature formation
Side A
1). Encrypt own message with personal private key
2). Next encrypt received sequence with open keys of side B

Side B
3). Decrypt received sequence at first we are using personal private keys
4). Continuing procedure of decryption with open keys of side A:
5). If the message is readable that it was not underwent modifications

Figure 1 - Process of formation developed scheme of authentication on the basis of Ford Fulkerson algorithm and El-Gamal scheme

In developed authentication scheme, a novelty is presented due to the fact that algorithms of maximum flow were not earlier used in cryptography. Also scheme of authentication were considered cryptographic endurable because those full selection attacks are completely excluded attacker do not have data regarding of size dimension of adjacency matrix (all adjacency matrix are stored in secured memory area of server and known only to client and server) as well edges weights (throughputs) of transport network can be changed during some time intervals (taking place operations of incrementing, decrementing on pre-installed values stipulated between each client). A scheme using not only tools of hashing but also the Electronic Digital Signature for proving that client calculated values of arbitrary blocking flows and maximum flow. Totally there are

$$\big((V*V)*(E*E)*(N*N)*(M*M)\big)/k$$

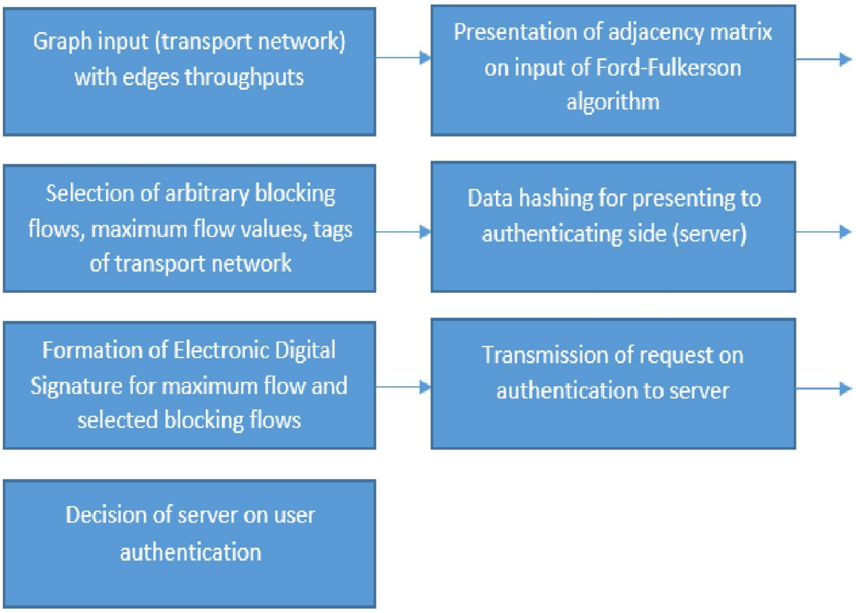
values for transport network of the adjacency matrix, V – number of vertexes, E- number of edges, N – bit capacity of used numbers in adjacency matrix, M – size of used numbers. k – number of attempts for presenting authentication data. Considering that attacker does not know closed keys of users and does not know in which order data are applied for forming Electronic Digital Signature cracking the following scheme is not possible.

P=19 – prime number

$$\{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18\}$$

Function of Euler totient. Primitive roots 2,3,10,13,14,15

$$Phi(19) = 18$$
$$Mod\ 19$$



Graph input (transport network) with edges throughputs

Presentation of adjacency matrix on input of Ford-Fulkerson algorithm

Selection of arbitrary blocking flows, maximum flow values, tags of transport network

Data hashing for presenting to authenticating side (server)

Formation of Electronic Digital Signature for maximum flow and selected blocking flows

Transmission of request on authentication to server

Decision of server on user authentication

Figure 2 - Scheme of the developed system

Table 1 - Primitive roots

x^i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
4	4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1
5	5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1
6	6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1
7	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1
8	8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1
9	9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	16	3
10	10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
11	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	10	15	11
12	12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1
13	13	17	12	4	14	11	10	16	18	6	2	7	15	5	11	15	9	12
14	14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	15	16	12	9	2	11	13	5	18	4	3	7	10	16	6	14	5	8
16	16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1
17	17	4	11	16	6	7	5	9	1	17	4	11	15	11	4	7	1	10
18	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	8	3

As primitive roots, such numbers are applicable which by multiplication by power of 2 from $x, x^2 \ldots . x^{18}$ and with division by modulus of 19 giving numbers from 1 to 18, those numbers are primitive roots [3,4].

(p, Gamm, Betta) – public key M = (Gamm, Betta) – signature

$$\alpha = 14$$
$$1 \le \mathrm{a} \le \mathrm{p} - 2$$
$$1 \le \mathrm{a} \le 17$$
$$\mathrm{a} = 12$$
$$\beta = 14^2 \bmod 19$$
$$\beta = 11$$
$$(\mathrm{p}, \alpha, \beta) = (19{,}14{,}11) - open\ key$$
$$\mathrm{M} = \mathrm{x} = 41$$
$$1 \le 4 \le \mathrm{p} - 2$$
$$1 \le \mathrm{r} \le 17$$
$$\gamma = \alpha^{\mathrm{r}} \bmod \mathrm{p}$$
$$\mathrm{r} = 13$$
$$\gamma = \alpha^{13} \bmod \mathrm{p} \quad \mathrm{x} = \mathrm{M} = 41$$
$$\gamma = 14^{13}\ mod\ 19 = 2$$
$$\delta = (41 - 12 * 2) * 13^{-1}\, mod\ 18$$
$$\delta = (17) * 13^{-1}\, mod\ 18$$
$$\delta = (17) * 7 = 119$$
$$\mathrm{M} = (\gamma, \delta) - signature\ M = (2{,}119)$$

Check

$$\delta^{\gamma} \gamma^{\delta} \equiv \alpha^{x}\ mod\ p$$
$$11^2\ 2^{119} \equiv 14^{41}\ mod\ 19 = 10$$

Checking that

$$\delta^{\gamma} \gamma^{\delta} \equiv \alpha^{x}\ mod\ p$$

$$11^2\ 2^{119} \equiv 14^{41}\ mod\ 19 = 10$$

Then the process of verification is accomplished.

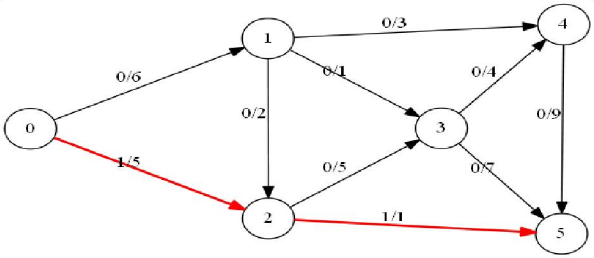
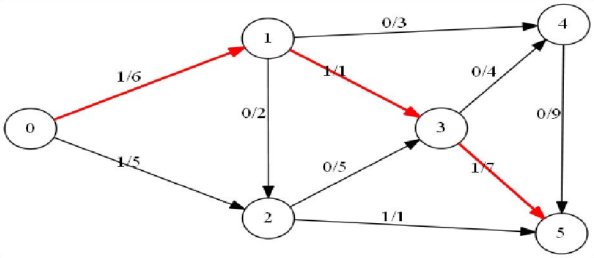
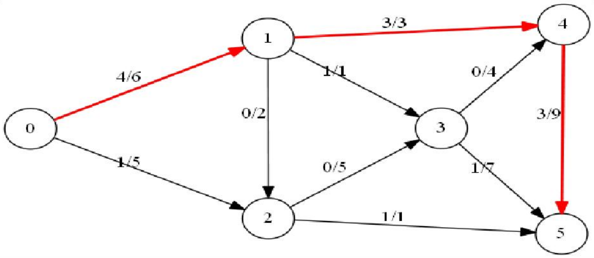
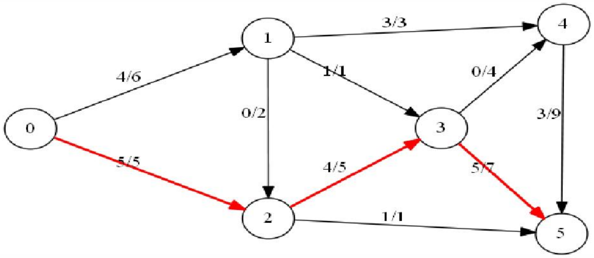
The algorithm of Ford-Fulkerson. A dynamic algorithm for finding the maximum flow in a transport network was developed in 1956 by mathematicians Lester Randolph Ford Jr. and Delbert Ray Fulkerson. The algorithm for finding the maximum flow concluded to search any path from s to t by dfs while such paths are existing.

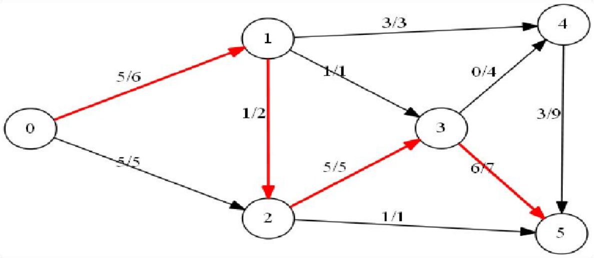
Non-formal description of the algorithm:

1. All flows are set to zero. The residual network initially is matching with the original transport network.
2. In residual network searching path from s to t, by dfs. If such path does not exist then the algorithm finishes its work.
3. On founded path passing maximal possible flow:
1. On given path in residual network searching edge with minimal capacity c_{min}.
2. For each edge in founded path incrementing the flow on c_{min}, in reverse direction decreasing on c_{min}.
3. The residual network is updating. For edges in the founded path and in reverse direction, a new throughput is calculated.
4. Return to step 2.

Table 2 - Tracing of the Ford-Fulkerson algorithm on transport network with 6 vertexes

All illustrations of oriented weighted graphs (transport networks) presented in SFDP notation.

	G
	 0 1 2 3 4 5 0/3 0/6 0/1 0/4 0/2 0/9 1/5 0/5 0/7 1/1
	Iteration description
	All flows are set to zero. The residual network initially is matched with the original transport network. Blocking flow on the 1st iteration of the Ford-Fulkerson algorithm consists of the following paths: 1. {0,2,5} 1 unit of flow
	G
	 0 1 2 3 4 5 0/3 1/6 1/1 0/4 0/2 0/9 1/5 0/5 1/7 1/1
	Iteration description
	Blocking flow on the 2nd iteration of the Ford-Fulkerson algorithm consists of the following paths: 2. {0,1,3,5} 8 units of flow
	G
	 0 1 2 3 4 5 3/3 4/6 1/1 0/4 0/2 3/9 1/5 0/5 1/7 1/1
	Iteration description
	Blocking flow on the 3rd iteration of the Ford-Fulkerson algorithm consists of the following paths: 1. {0,1,4,5} 3 units of flow
	G
	 0 1 2 3 4 5 3/3 4/6 1/1 0/4 0/2 3/9 5/5 4/5 5/7 1/1
	Iteration description
	Blocking flow on the 4th iteration of the Ford-Fulkerson algorithm consists of the following paths: 1. {0,2,3,5} 4 units of flow
	G

	 0 1 2 3 4 5 5/6 5/5 3/3 1/1 1/2 0/4 3/9 5/5 6/7 1/1
	Iteration description
	Blocking flow on 5th iteration of Ford-Fulkerson algorithm consists of following paths: 1. {0,1,2,3,5} 1 unit of flow, Maximum flow $\|f\|$ equals 10.

Symmetric block encryption algorithm Blowfish with key dependable S blocks of substitution. Optionally the 3rd trusted side could use block symmetric cipher for encrypting packets with open keys. Symmetric block cipher Blowfish is one of a kind cipher based on Feistel network and wherein having key dependable S blocks. Symmetric block cipher Blowfish have an unaccustomed size of key in 448 bits for symmetric block ciphers which is more inherent to stream ciphers like A5-1, RC-4 [5].

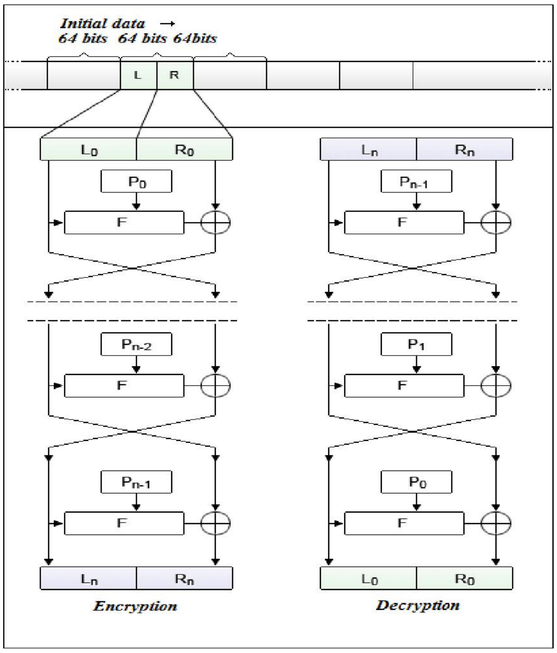


Figure 3 - Scheme of Blowfish algorithm

Function F(X)

1. 32 bits input data are divided into 4 8 bits blocks (X_1, X_2, X_3, X_4). Each of that blocks are indexed by numbers of S blocks $S_1 - S_4$
2. On values $S_1[X_1], S_2[X_2]$ conducting addition by modulus of 2^{32}, also on values $S_3[X_3], S_4[X_4]$ conducting addition by modulus 2^{32}
3. Results of that operations are output values of function F(X)

Formation of round keys

1. Arrays P, S initializing with the help of secret key K
2. Values $P_1 - P_{18}$ initialized by fixed string of hexadecimal representation of Pi number.
3. Operation XOR conducted on array P_i with first 32 bits of key K. Next with second 32 bits and so on.

Encryption of keys and substitution tables of S-blocks

1. Occurring alternate encryption, initial encrypted value 64 bits zero string. Results are written in values of $P_1 - P_{18}$, $S_1 - S_4$, following operations occurring until all values of $P_1 - P_{18}$, $S_1 - S_4$ would be not formed.

Appliance of blocking flow in steganography, LSB algorithm. If a following blocking flow {0,1,2,3,5} is used then writing data: 01011 would be performing at zero, first, second, third and fifth LSB bite of media container:

0100101**0** 0110101**1** 0110101**0** 0101101**1** 01001000 0100100**1** 00001010

Conclusion. Not all systems of Digital Electronic Signatures require additional confirmation factors of sides, insertion of output data of the Ford-Fulkerson algorithm (blocking flow, transport network) improves the security of Electronic Digital Signature. Due to the fact that transport network by itself is not encrypted by El-Gamal algorithm but hashes this allows to reduce the amount of data for encryption to increase performance and data of blocking flow, transport network would be serving not as key but the kind of client identification tags participants of data transmission channel.

REFERENCES

[1] S. Singh. Book of ciphers. M.: Astrel, **2006**. 447 pp.

[2] Schneier B. Applied cryptography. M.: Williams, **2002**. 816 pp.

[3] Wenbo M. Modern cryptography. M.: Williams, **2005**. 297 pp.

[4] Yashchenko V.V. Cryptography introduction. M.: MCNOM: CheRo, **2000**. 287 pp.

[5] Moldovyan N.A. Cryptography with public key. SPb.: BHV, **2004**. 288 pp.

А.А. Жатқанбаев

Әл-Фараби атындағы Қазақ ұлттық университеті

АҚПАРАТТЫ СТЕГЕОГРАФИЯЛЫҚ ҚОРҒАУДЫҢ ЖӘНЕ АУТЕНТИФИКАЦИЯ ТИІМДІ СХЕМАСЫ МАКСИМАЛДЫ АҒЫНДЫ ТАБУДЫҢ АЛГОРИТМДЕРІ НЕГІЗІНДЕ

Аннотация. Эль-Гамаль алгоритміне негізделген электрондық цифрлық қолтаңбаның тиімді схемасын әзірледі, көлік желісі және оңы ағынды блоктау (шығыс деректері) Форд-Фалкерсон максималды ағынын табудың алгоритмдері тараптардың аутентификациясы үшін қосымша деректер ретінде қызмет етеді. Көлік желісі және ағынды блоктау қосылған сұлба тиімді деп саналады өйткені көптеген ұқсас блоктау ағындар және түрлі көлік желілері болуы мүмкін осы ағындармен байланысты.

Түйін сөздер. стеганография, Форд-Фалкерсон алгоритм, ағынды блоктау, криптография, ағым, аутентификация.

А.А. Жатқанбаев

Казахский национальный университет имени Аль-Фараби

ЭФФЕКТИВНАЯ СХЕМА СТЕГАНОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ И АУТЕНТИФИКАЦИИ НА ОСНОВЕ АЛГОРИТМОВ НАХОЖДЕНИЯ МАКСИМАЛЬНОГО ПОТОКА

Аннотация. Разработанная эффективная схема электронной цифровой подписи, на основе алгоритма Эль-Гамаля, транспортная сеть и ее блокирующие потоки (выходные данные) произведенные алгоритмом нахож-дения максимального потока Форда-Фалкерсона служат дополнительными данными для аутентификации сторон. Схема с добавлением транспортных сетей и их блокирующих потоков считается эффективной так как может существовать множество одинаковых блокирующих потоков и различных транспортных сетей, ассоциированных с данными потоками.

Ключевые слова: стеганография, алгоритм Форда-Фалкерсона, блокирующий поток, криптография, поток, аутентификация.

Zhatkanbayev Almas Altayuly – bachelor of technics and technology by specialty 5B070400 «Computer systems and software», Al-Farabi Kazakh National University, master student of 2nd course of specialty 6M100200 «Systems of information security», +7(727)-262-15-78, +7(777)-254-33-50, wildlife.kz@gmail.com