

ISSN 2518-1483 (Online),
ISSN 2224-5227 (Print)

2018 • 2

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫНЫҢ

БАЯНДАМАЛАРЫ

ДОКЛАДЫ

НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК
РЕСПУБЛИКИ КАЗАХСТАН

REPORTS

OF THE NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN

ЖУРНАЛ 1944 ЖЫЛДАН ШЫҒА БАСТАҒАН
ЖУРНАЛ ИЗДАЕТСЯ С 1944 г.
PUBLISHED SINCE 1944



Бас редакторы
х.ғ.д., проф., ҚР ҰҒА академигі **М.Ж. Жұрынов**

Редакция алқасы:

Адекенов С.М. проф., академик (Қазақстан) (бас ред. орынбасары)
Величкин В.И. проф., корр.-мүшесі (Ресей)
Вольдемар Вуйцик проф. (Польша)
Гончарук В.В. проф., академик (Украина)
Гордиенко А.И. проф., академик (Белорус)
Дука Г. проф., академик (Молдова)
Илолов М.И. проф., академик (Тәжікстан),
Леска Богуслава проф. (Польша),
Локшин В.Н. проф. чл.-корр. (Қазақстан)
Нараев В.Н. проф. (Ресей)
Неклюдов И.М. проф., академик (Украина)
Нур Изура Удзир проф. (Малайзия)
Перни Стефано проф. (Ұлыбритания)
Потапов В.А. проф. (Украина)
Прокопович Полина проф. (Ұлыбритания)
Омбаев А.М. проф., корр.-мүшесі (Қазақстан)
Өтелбаев М.О. проф., академик (Қазақстан)
Садыбеков М.А. проф., корр.-мүшесі (Қазақстан)
Сатаев М.И. проф., корр.-мүшесі (Қазақстан)
Северский И.В. проф., академик (Қазақстан)
Сикорски Марек проф. (Польша)
Рамазанов Т.С. проф., академик (Қазақстан)
Такибаев Н.Ж. проф., академик (Қазақстан), бас ред. орынбасары
Харин С.Н. проф., академик (Қазақстан)
Чечин Л.М. проф., корр.-мүшесі (Қазақстан)
Харун Парлар проф. (Германия)
Энджун Гао проф. (Қытай)
Эркебаев А.Э. проф., академик (Қырғыстан)

«Қазақстан Республикасы Ұлттық ғылым академиясының баяндамалары»

ISSN 2518-1483 (Online),

ISSN 2224-5227 (Print)

Меншіктенуші: «Қазақстан Республикасының Ұлттық ғылым академиясы» Республикалық қоғамдық бірлестігі (Алматы қ.)
Қазақстан республикасының Мәдениет пен ақпарат министрлігінің Ақпарат және мұрағат комитетінде 01.06.2006 ж.
берілген №5540-Ж мерзімдік басылым тіркеуіне қойылу туралы куәлік

Мерзімділігі: жылына 6 рет.

Тиражы: 500 дана.

Редакцияның мекенжайы: 050010, Алматы қ., Шевченко көш., 28, 219 бөл., 220, тел.: 272-13-19, 272-13-18,
http://nauka-nanrk.kz_reports-science.kz

© Қазақстан Республикасының Ұлттық ғылым академиясы, 2018

Типографияның мекенжайы: «Аруна» ЖК, Алматы қ., Муратбаева көш., 75.

Главный редактор
д.х.н., проф., академик НАН РК **М. Ж. Журинов**

Редакционная коллегия:

Адекенов С.М. проф., академик (Казахстан) (зам. гл. ред.)
Величкин В.И. проф., чл.-корр. (Россия)
Вольдемар Вуйцик проф. (Польша)
Гончарук В.В. проф., академик (Украина)
Гордиенко А.И. проф., академик (Беларусь)
Дука Г. проф., академик (Молдова)
Илолов М.И. проф., академик (Таджикистан),
Леска Богуслава проф. (Польша),
Локшин В.Н. проф. чл.-корр. (Казахстан)
Нараев В.Н. проф. (Россия)
Неклюдов И.М. проф., академик (Украина)
Нур Изура Удзир проф. (Малайзия)
Перни Стефано проф. (Великобритания)
Потапов В.А. проф. (Украина)
Прокопович Полина проф. (Великобритания)
Омбаев А.М. проф., чл.-корр. (Казахстан)
Отелбаев М.О. проф., академик (Казахстан)
Садыбеков М.А. проф., чл.-корр. (Казахстан)
Сатаев М.И. проф., чл.-корр. (Казахстан)
Северский И.В. проф., академик (Казахстан)
Сикорски Марек проф., (Польша)
Рамазанов Т.С. проф., академик (Казахстан)
Такибаев Н.Ж. проф., академик (Казахстан), зам. гл. ред.
Харин С.Н. проф., академик (Казахстан)
Чечин Л.М. проф., чл.-корр. (Казахстан)
Харун Парлар проф. (Германия)
Энджун Гао проф. (Китай)
Эркебаев А.Э. проф., академик (Кыргызстан)

Доклады Национальной академии наук Республики Казахстан»

ISSN 2518-1483 (Online),

ISSN 2224-5227 (Print)

Собственник: Республиканское общественное объединение «Национальная академия наук Республики Казахстан» (г. Алматы)

Свидетельство о постановке на учет периодического печатного издания в Комитете информации и архивов Министерства культуры и информации Республики Казахстан №5540-Ж, выданное 01.06.2006 г.

Периодичность: 6 раз в год.

Тираж: 500 экземпляров

Адрес редакции: 050010, г.Алматы, ул.Шевченко, 28, ком.218-220, тел. 272-13-19, 272-13-18

<http://nauka-nanrk.kz> reports-science.kz

©Национальная академия наук Республики Казахстан, 2018 г.

Адрес типографии: ИП «Аруна», г.Алматы, ул.Муратбаева, 75

E d i t o r i n c h i e fdoctor of chemistry, professor, academician of NAS RK **M.Zh. Zhurinov****E d i t o r i a l b o a r d :****Adekenov S.M.** prof., academician (Kazakhstan) (deputy editor in chief)**Velichkin V.I.** prof., corr. member (Russia)**Voitsik Valdemar** prof. (Poland)**Goncharuk V.V.** prof., academician (Ukraine)**Gordiyenko A.I.** prof., academician (Belarus)**Duka G.** prof., academician (Moldova)**Ilolov M.I.** prof., academician (Tadjikistan),**Leska Boguslava** prof. (Poland),**Lokshin V.N.** prof., corr. member. (Kazakhstan)**Narayev V.N.** prof. (Russia)**Nekludov I.M.** prof., academician (Ukraine)**Nur Izura Udzir** prof. (Malaysia)**Perni Stephano** prof. (Great Britain)**Potapov V.A.** prof. (Ukraine)**Prokopovich Polina** prof. (Great Britain)**Ombayev A.M.** prof., corr. member. (Kazakhstan)**Otelbayv M.O.** prof., academician (Kazakhstan)**Sadybekov M.A.** prof., corr. member. (Kazakhstan)**Satayev M.I.** prof., corr. member. (Kazakhstan)**Severskyi I.V.** prof., academician (Kazakhstan)**Sikorski Marek** prof., (Poland)**Ramazanov T.S.** prof., academician (Kazakhstan)**Takibayev N.Zh.** prof., academician (Kazakhstan), deputy editor in chief**Kharin S.N.** prof., academician (Kazakhstan)**Chechin L.M.** prof., corr. member. (Kazakhstan)**Kharun Parlar** prof. (Germany)**Endzhun Gao** prof. (China)**Erkebayev A.Ye.** prof., academician (Kyrgyzstan)**Reports of the National Academy of Sciences of the Republic of Kazakhstan.****ISSN 2224-5227****ISSN 2518-1483 (Online),****ISSN 2224-5227 (Print)**

Owner: RPA "National Academy of Sciences of the Republic of Kazakhstan" (Almaty)

The certificate of registration of a periodic printed publication in the Committee of Information and Archives of the Ministry of Culture and Information of the Republic of Kazakhstan N 5540-Ж, issued 01.06.2006

Periodicity: 6 times a year

Circulation: 500 copies

Editorial address: 28, Shevchenko str., of.219-220, Almaty, 050010, tel. 272-13-19, 272-13-18,

<http://nauka-nanrk.kz> / reports-science.kz

**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 durable 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

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

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

$$\text{Phi}(19) = 18 \\ \text{Mod } 19$$

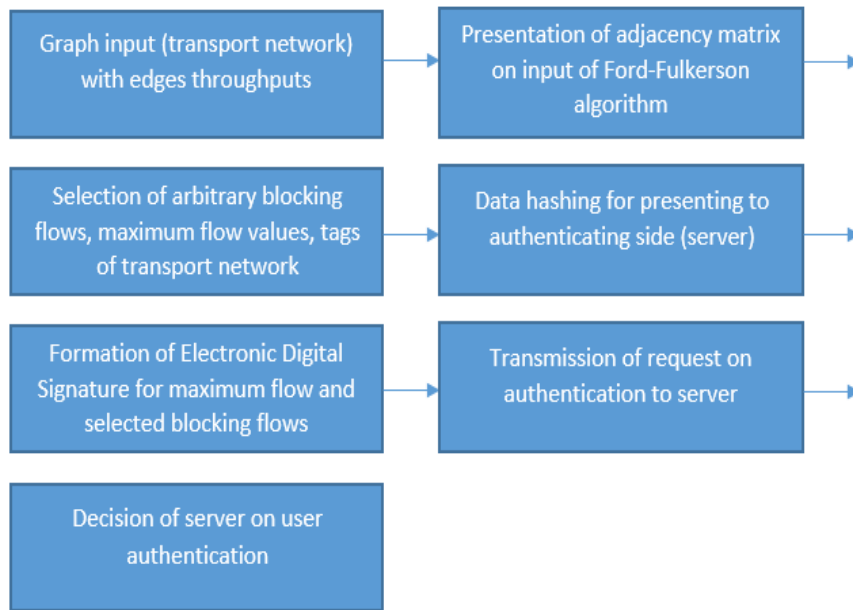


Figure 2 - Scheme of the developed system

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	17	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 $x, x^2 \dots x^{18}$ 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

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

Check

$$\begin{aligned}
 \delta^r \gamma^\delta &\equiv \alpha^x \bmod p \\
 11^2 2^{119} &\equiv 14^{41} \bmod 19 = 10
 \end{aligned}$$

Checking that

$$\begin{aligned}
 \delta^r \gamma^\delta &\equiv \alpha^x \bmod p \\
 11^2 2^{119} &\equiv 14^{41} \bmod 19 = 10
 \end{aligned}$$

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.

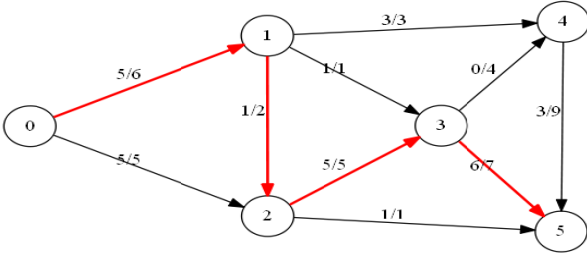
Non-formal description of the algorithm:

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

	
	Iteration description
	Blocking flow on 5 th 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].

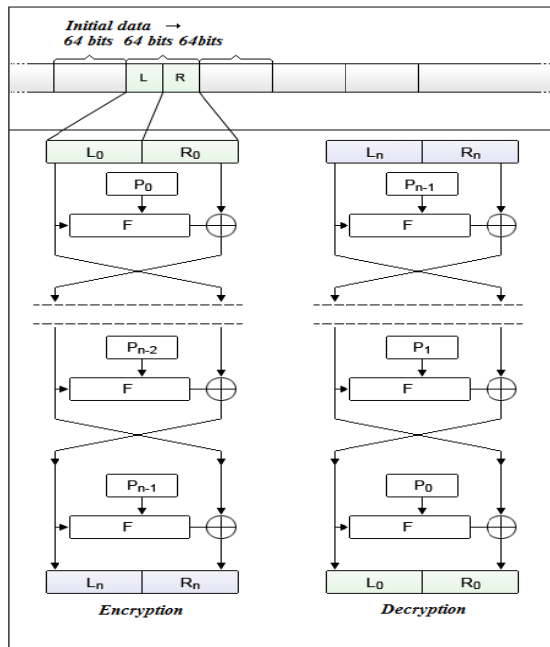


Figure 3 - Scheme of Blowfish algorithm

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:

01001010 01101011 01101010 01011011 01001000 01001001 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-Гамала, транспортная сеть и ее блокирующие потоки (выходные данные) произведенные алгоритмом нахождения 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

МАЗМҰНЫ

Техникалық ғылымдар

(ағылшын тілінде)

<i>Генбач А.А., Шоколаков К.К.</i> Көбік өндіретін және көбік сөндіретін құрылымдармен бүркігішсіз капиллярлы-кеуекті тозан-газ тұтқыштарды әзірлеу.....	5
<i>Ермағамбет Б.Т., Қазанқанова М.Қ., Ермағамбетов Ж.Х., Наурызбаева А.Т., Канағатов К.Г., Абылғазина Л.Д.</i> Көміртектегі наноталшықтарды таскөмір пегінен алу әдістері.....	9
<i>Жатқанбаев А.А.</i> Ақпаратты стегеографиялық қорғаудың және аутентификация тиімді схемасы максималды ағынды табудың алгоритмдері негізінде.....	17
<i>Ахметов Б.</i> Қазақстан көлігінің ақпараттық-коммуникациялық жүйелерінің киберқауіпсіздігінің күйі, болашағы және негізгі бағыттары.....	23
<i>Казенова А.О., Бренер А.М., Голубев В.Г., Кенжалиева Г.Д., Шапалов Ш.К., Бекаулова А.А.</i> Кластерлеу немесе агрегаттаумен технологиялық жүйелердің математикалық модельдерін талдау.....	31
<i>Құралбаев З. Қ.</i> Тұтқырлы қабаттың материалдарының қырат баурайына төмен түсуі туралы есепті шешу.....	36
<i>Нұртай Ж.Т., Наукенова А.С., Досалиев Қ.С., Жорабек А.А., Шапалов Ш.К.</i> Селден қорғайтын қорғаныс құрылымдары үшін бастапқы шикізаттарды таңдау	43
<i>Тәтенов А.М., Жүнісбекова А.С.</i> Толқындық оптика құбылыстарының математикалық байланыстар алгоритмін Flash-CC, Java script-бағдарлау орталарында интербелсенді виртуалдау.....	47

Аграрлық ғылымдар

(ағылшын тілінде)

<i>Әкімбаев А.Р., Баймұқанов Д.А., Исхан Қ.Ж., Омаров М.М., Әубәкіров Х.А.</i> Әртүрлі түрлі генотиптегі биелердің сүттілігі және сүт құрамы.....	54
<i>Омбаев Ә., Тамаровский М., Даниленко О., Қарымсақов Т.</i> Етті бағыттағы мал шаруашылығындағы селекциялық – асылдандыру жұмысының кейбір қырлары.....	63

Қоғамдық ғылымдар

(ағылшын тілінде)

<i>Закирова М. С., Алан Р.</i> ЕУРАЗЭҚ-тың қалыптасуы мен дамуының негізгі үрдістері: интеграциялану мәселелері мен болашағы.....	68
<i>Есенбекова Ә. Б., Роберт Алан.</i> Жасыл экономика тұрақты дамудың жаңа бағыты ретінде.....	72
<i>Шалкибаева. Ж.А., Утеев Б. Ж.</i> Аймақтардың салықтық әлеуетін бағалаудың әдістемелік құралдары.....	79
<i>Ахметжанов Б., Тәжібекова К.Б., Шаметова А.А.</i> Елдің инновациялық экономикасы: проблемалары және олардың шешімдерінің жолдары.....	86
<i>Ахметова А.С., Рахимбекова А.Е., Болтаева А.А., Махатова А.Б.,</i> Экологиялық менеджменттің жауапкершілікті бизнесті басқару жолы.....	90
<i>Аюпова З.К., Құсайынов Д.Ө.</i> Интеграциялық процесстердің орталық Азия елдерінің құқықтық жүйесіне тигізетін әсерлері.....	96
<i>Байкин А.К., Шалболова Е.Ж., Тарануха Ю.В.</i> Дивидификация инновациялық секторларды дамыту факторы.....	102
<i>Ескадиева А.Ж., Әдиетова Е.М., Рахимова С.А.</i> Экономиканы жаңғырту жағдайында адам капиталы.....	108
<i>Исаева Б.К., Тлесова Э.Б., Азатбек Т.А.</i> Шетелдік мұнай компанияларының кадрлық әлеуетінің инновациялық даму ерекшеліктері және олардың тәжірибесін Қазақстанда пайдалану.....	112
<i>Кемел М., Бакирбекова А.М., Таштанова Н.Н.</i> Қазақстандық компаниялардың басқару жүйесіндегі корпоративтік әлеуметтік жауапкершілік	121
<i>Мукушева Г.К., Ондашова А.Ж.</i> Токсикалық металдардың ион және тиістік металдардың тоқтатуға арналған золотель және читосанға негізді тыйымдар.....	127
<i>Ламбекова А.Н., Нурғалиева А.М.</i> Екінші деңгейлі банктердің ішкі аудитінде ақпараттық технологиялы қолдану қажеттілігі	131
<i>Сабирова Р.К., Кирдасинова К.А., Дингазиева М.Д., Жұмағұлова М.М., Луқпанова М.А.</i> Кәсіпорындағы жұмысшылардың компаниясы жүйесін жетілді.....	135
<i>Саябаев К.М., Абдрахманова Р.С., Дошан А.С., Мукашева Г.М.</i> Ақмолының айылық саласындағы ұрақты дамудың әдістемесіне әдістемелік бағыттар METHODOLOGICAL.....	139
<i>Умирзаков С.Ы., Наурызбаев А.Ж., Бұхарбаева А.Ж.</i> Күрішөндірісін мемлекеттік қолдау тиімділігін арттыру – Қазақстанның агроөнеркәсіптік кешенінің даму стратегиясының негізі.....	144

<i>Хуаныш Л. Кәсіпорын басқару жүйесінің ішкі бақылауының рөлі.....</i>	153
<i>Жумабаев А.К., Магай Т.П., Пол Мартин. Қазақстанның сүт өнеркәсібі тиімді бизнес үлгісін іздеуде.....</i>	159

Техникалық ғылымдар

(орыс тілінде)

<i>Генбач А.А., Шоколаков К.К. Көбік өндіретін және көбік сөндіретін құрылымдармен бүркігішсіз капиллярлы-кеуекті тозаң-газ тұтқыштарды әзірлеу.....</i>	167
--	-----

Аграрлық ғылымдар

(орыс тілінде)

<i>Әкімбаев А.Р., Баймұқанов Д.А., Исхан Қ.Ж., Омаров М.М., Әубәкіров Х.А. Әртүрлі түрлі генотиптегі биелердің сүттілігі және сүт құрамы.....</i>	172
---	-----

<i>Омбаев Ә., Тамаровский М., Даниленко О., Қарымсақов Т. Етті бағыттағы мал шаруашылығындағы селекциялық – асылдандыру жұмысының кейбір қырлары.....</i>	181
---	-----

Қоғамдық ғылымдар

(орыс тілінде)

<i>Жумабаев А.К., Магай Т.П., Пол Мартин. Қазақстанның сүт өнеркәсібі тиімді бизнес үлгісін іздеуде.....</i>	186
<i>Шалкибаева. Ж.А., Утеев Б. Ж. Аймақтардың салықтық әлеуетін бағалаудың әдістемелік құралдары.....</i>	195

СОДЕРЖАНИЕ

Технические науки

(на английском языке)

<i>Генбач А.А., Шоколаков К.К.</i> Разработка безфорсуночных капиллярно-пористых пылегазоуловителей с пеногенерирующими и пеногасящими структурами.....	5
<i>Ермагамбет Б.Т., Казанкапова М.К., Ермагамбетов Ж.Х., Наурызбаева А.Т., Канагатов К.Г., Абылгазина Л.Д.</i> Методы получения углеродных нановолокон из каменноугольного ПЕКА.....	9
<i>Жатқанбаев А.А.</i> Эффективная схема стеганографической защиты информации и аутентификации на основе алгоритмов нахождения максимального потока	17
<i>Ахметов Б.</i> Состояние, перспективы и основные направления развития кибербезопасности информационно-коммуникационных систем транспорта Казахстана.....	23
<i>Казенова А.О., Бренер А.М., Голубев В.Г., Кенжалиева Г.Д., Шапалов Ш.К., Бекаулова А.А.</i> Анализ математических моделей технологических систем с кластеризацией или агрегацией.....	31
<i>Куралбаев З. К.</i> Решение задачи об опускании материалов вязкого слоя по склону возвышенности	36
<i>Нуртай Ж.Т., Наукенова А.С., Досалиев К.С., Жорабек А.А., Шапалов Ш.К.</i> Подбор исходных шихтовых материалов для селезащитных конструкций	43
<i>Татенов А.М., Жунибекова А.С.</i> Интерактивная виртуализация в среде Flash-CC, Java script алгоритмов математических связей явления волновой оптики.....	47

Аграрные науки

(на английском языке)

<i>Акимбеков А.Р., Баймуканов Д.А., Исхан К.Ж., Омаров М.М., Аубакиров Х.А.</i> Молочная продуктивность и состав молока кобыл разных генотипов.....	54
<i>Омбаев А., Тамаровский М., Даниленко О., Карымсаков Т.</i> Некоторые аспекты селекционно-племенной работы в мясном скотоводстве	63

Общественные науки

(на английском языке)

<i>Закирова М.С., Алан Р.</i> Основные тенденции образования и развития ЕВРАЗЭС: проблемы и перспективы интеграции.....	68
<i>Есенбекова А.Б., Роберт Алан.</i> Зеленая экономика как новый путь устойчивого развития.....	72
<i>Шалжибаева Ж.А., Утеев Б. Ж.</i> Методический инструментарий оценки налогового потенциала региона.....	79
<i>Ахметжанов Б., Тажиббекова К.Б., Шаметова А.А.</i> Инновационная экономика страны: проблемы и пути их решения.....	86
<i>Ахметова А.С., Рахимбекова А.Е., Болтаева А.А., Махатова А.Б.</i> Экологический менеджмент как путь к ответственному ведению бизнеса	90
<i>Аюпова З.К., Кусаинов Д.У.</i> Влияние интеграционных процессов на развитие правовых систем стран Центральной Азии.....	96
<i>Байкин А.К., Шальболова Ю.Ж., Тарануха Ю.В.</i> Диверсификация как фактор в развитии инновационных секторов экономики.....	102
<i>Ескалиева А.Ж., Адиева Э.М., Рахимова С.А.</i> Человеческий капитал в условиях модернизации экономики.....	108
<i>Исаева Б.К., Глесова Э.Б., Азатбек Т.А.</i> Особенности инновационного развития кадрового потенциала зарубежных нефтяных компаний и применения их опыта в Казахстане.....	112
<i>Кемел М., Бакирбекова А.М., Таишанова Н.Н.</i> Корпоративная социальная ответственность в системе управления казахстанских компаний	121
<i>Мукушева Г.К., Ондашова А.Ж.</i> Сорбционные материалы на основе цеолита и хитозана для обезвреживания ионов токсичных металлов.....	127
<i>Ламбекова А.Н., Нургалиева А.М.</i> Необходимость применения информационных технологий во внутреннем аудите в банках второго уровня.....	131
<i>Сабирова Р.К., Кирдасинова К.А., Дингазиева М.Д., Жумагулова М.М., Луқпанова М.А.</i> Совершенствование системы вознаграждения работников на предприятии.....	135
<i>Саябаев К.М., Абдрахманова Р.С., Дошан А.С., Мукашева Г.М.</i> Методические подходы к оценке устойчивого развития сельских территорий акмолинской области.....	139
<i>Умирзаков С.Ы., Наурызбаев А.Ж., Бұхарбаева А.Ж.</i> Повышение эффективности государственной поддержки рисоводства – основа стратегии развития агропромышленного комплекса Казахстана.....	144

<i>Хуаныш Л.</i> Роль внутреннего контроля в системе управления предприятием.....	153
<i>Жумабаев А.К., Магай Т.П., Пол Мартин.</i> Молочная отрасль Казахстана в поиске эффективной бизнес модели....	159
Технические науки (на русском языке)	
<i>Генбач А.А., Шоколаков К.К.</i> Разработка безфорсуночных капиллярно-пористых пылегазоуловителей с пеногенерирующими и пеногасящими структурами.....	167
Аграрные науки (на русском языке)	
<i>Акимбеков А.Р., Баймуканов Д.А., Исхан К.Ж., Омаров М.М., Аубакиров Х.А.</i> Молочная продуктивность и состав молока кобыл разных генотипов.....	172
<i>Омбаев А., Тамаровский М., Даниленко О., Карымсаков Т.</i> Некоторые аспекты селекционно-племенной работы в мясном скотоводстве	181
Общественные науки (на русском языке)	
<i>Жумабаев А.К., Магай Т.П., Пол Мартин.</i> Молочная отрасль Казахстана в поиске эффективной бизнес модели.....	186
<i>Шалжибаева Ж.А., Утеев Б. Ж.</i> Методический инструментарий оценки налогового потенциала региона.....	195

CONTENTS
Technical sciences

(in English)

<i>Genbach A.A., Skokolakov K.K.</i> Development of nozzle-free capillary porous dust-and-gas collectors with foam generating and defoaming structures.....	5
<i>Ermagambet B.T., Kazankapova M.K., Ermogambetov Zh.Kh., Nauryzbayeva A.T., Kanagatov K.G., Abylgazina L.D.</i> Methods for producing carbon nanofibers from coal pitch.....	9
<i>Zhatkanbayev A.A.</i> Effective scheme of steganography information protection and authentication based on maximum flow algorithms	17
<i>Akhmetov B.</i> Status, perspectives and main directions of the development of cybersecurity of information and communication transport systems of Kazakhstan.....	23
<i>Kazenova A., Brener A., Golubev V., Kenzhalieva G., Shapalov Sh., Bekaulova A.A.</i> Analysis of mathematical models of technological systems with clustering or aggregation.....	31
<i>Kuralbayev Z. K.</i> Solution of the problem of lowering of materials of viscous layer down the hillslope.....	36
<i>Nurtay Zh.T., Naukenova A.S., Dosaliyev K.S., Zhorabek A.A., Shapalov Sh.K.</i> Selection of initial charge materials for mud protection structures	43
<i>Tatenov A.M., Zhunisbekova A.S.</i> Interactive virtualization in the environment of flash-cc, java script of algorithms of mathematical communications the phenomenon of wave optics.....	47

Agrarian science

(in English)

<i>Akimbekov A.R., Baimukanov D.A., Iskhan K.Zh., Omarov M.M., Aubakirov Kh.A.</i> Dairy productivity and milk composition of mares of different genotypes.....	54
<i>Ombaev A., Tamarovsky M., Danilenko O., Karymsakov T.</i> Some aspects of selection-breeding work in meat cattle breeding.....	63

Social Sciences

(in English)

<i>Zakirova M.S., Alan R.</i> The main tendencies of the creation and development of eurasian economic UNION: problems and prospects of integration.....	68
<i>Esenbekova A.B., Robert Alan.</i> Green economy as the new way of sustainable development.....	72
<i>Shalkibayeva Zh. A., Uteyev B.Zh.</i> Methodical toolkit of regional tax potential assesment.....	79
<i>Akhmetzhanov B., Tazhibekova KB, Shametova A.A.</i> Innovative economy of the country: problems and the ways of their solutions.....	86
<i>Akhmetova A., Rakhimbekova A., Boltayeva A., Makhatova A.</i> Ecological management as the way to responsible business operation.....	90
<i>Ayupova Z.K., Kussainov D.U.</i> Influence of integration processes on the development of the legal systems of the central Asia countries	96
<i>Baikin A.K., Shalbolova Y.Zh., Taranukha Y.V.</i> Diversification as a factor in the development of innovative sectors.....	102
<i>Eskalieva A.Zh., Adietova E.M., Rakhimova S.A.</i> Human capital in the conditions of modernization of economics.....	108
<i>Issayeva B.K., Tlessova E.B., Azatbek T.A.</i> Peculiarities of innovative development of the personnel potential of foreign oil companies and application of their experience in Kazakhstan.....	112
<i>Kemel M., Tashtanova N.N., Bakirbekova A.M.</i> Corporate social responsibility in management systems of Kazakhstan companies	121
<i>Mukusheva G.K., Ondashova A.Zh.</i> Sorption materials based on zeolite and chitosane for the discharge of ions of toxic metals.....	127
<i>Lambekova A.N., Nurgaliyeva A.M.</i> Need of using of information technology in inner audit in the banks of the second level.....	131
<i>Sabirova R.K., Kirdasinova K.A., Dingazieva M.D., Zhumalova M.M., Lukpanova M.A.</i> Improvement of the compensation system for employees at the enterprise.....	135
<i>Sayabayev K.M.¹, Abdrakhmanova R.S.², Doshan A.S.³, Mukasheva G.M.</i> Approaches to estimation of sustainable development of rural areas of akmolin area.....	139
<i>Umirzakov S. I., Nauryzbayev A. Zh., Bukharbayeva A. Zh.</i> Improving efficiency of the state support of rice planting – baseline for the strategy of agro-industrial complex development in Kazakhstan.....	144
<i>Huanysh L.</i> Place of the internal control in management system and the form of its organization.....	153

<i>Zhumabayev A.K., Magay T.P.¹, Pohl Martin.</i> The search for the efficient business model for the dairy sector in Kazakhstan.....	159
--	-----

Technical sciences

(in Russian)

<i>Genbach A.A., Skokolakov K.K.</i> Development of nozzle-free capillary porous dust-and-gas collectors with foam generating and defoaming structures.....	167
---	-----

Agrarian science

(in Russian)

<i>Akimbekov A.R., Baimukanov D.A., Iskhan K.Zh., Omarov M.M., Aubakirov Kh.A.</i> Dairy productivity and milk composition of mares of different genotypes.....	172
---	-----

<i>Ombaev A., Tamarovsky M., Danilenko O., Karymsakov T.</i> Some aspects of selection-breeding work in meat cattle breeding.....	181
---	-----

Social Sciences

(in Russian)

<i>Zhumabayev A.K., Magay T.P.¹, Pohl Martin.</i> The search for the efficient business model for the dairy sector in Kazakhstan.....	186
--	-----

<i>Shalkibayeva Zh. A., Uteyev B.Zh.</i> Methodical toolkit of regional tax potential assessment.....	195
---	-----

**Publication Ethics and Publication Malpractice
in the journals of the National Academy of Sciences of the Republic of Kazakhstan**

For information on Ethics in publishing and Ethical guidelines for journal publication see <http://www.elsevier.com/publishingethics> and <http://www.elsevier.com/journal-authors/ethics>.

Submission of an article to the National Academy of Sciences of the Republic of Kazakhstan implies that the work described has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see <http://www.elsevier.com/postingpolicy>), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any other language, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The National Academy of Sciences of the Republic of Kazakhstan follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the originality detection service Cross Check <http://www.elsevier.com/editors/plagdetect>.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the National Academy of sciences of the Republic of Kazakhstan.

The Editorial Board of the National Academy of sciences of the Republic of Kazakhstan will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайте:

www.nauka-nanrk.kz

ISSN 2518-1483 (Online), ISSN 2224-5227 (Print)

<http://www.reports-science.kz/index.php/ru/>

Редакторы *М. С. Ахметова, Т.А. Апендиев, Аленов Д.С.*
Верстка на компьютере *А.М. Кульгинбаевой*

Подписано в печать 13.04.2018.
Формат 60x881/8. Бумага офсетная. Печать – ризограф.
12,6 п.л. Тираж 500. Заказ 2.