Improved Secure Stream Cipher for Cloud Computing

Sergiy Gnatyuk[1,2,3] [0000-0003-4992-0564], Maksim Iavich[4] [0000-0002-3109-7971], Vasyl Kinzeryavyy[1] [0000-0002-7697-1503], Tetyana Okhrimenko[1] [0000-0001-9036-6556], Yuliia Burmak[5] [0000-0002-5410-6260] and Iuliia Goncharenko[6] [0000-0002-5608-4632]

[1] National Aviation University, Kyiv, Ukraine
[2] State Scientific and Research Institute of Cybersecurity Technologies and Information Protection, Kyiv, Ukraine
[3] Yessenov University, Aktau, Kazakhstan
[4] Scientific Cyber Security Association, Tbilisi, Georgia
[5] Kyiv College of Communication, Kyiv, Ukraine
[6] European University, Kyiv, Ukraine
s.gnatyuk@nau.edu.ua, m.iavich@scsa.ge, v.kinzeryavyy@nau.edu.ua, taniazhm@gmail.com, burmak.yu@ukr.net, goncharenkoyuyu@gmail.com

Abstract. Today cloud services have revolutionized the way we store and share different data. At the same time, most of the data are unsecured and vulnerable to various cyberattacks. In this paper cloud services concept and mechanisms of their work were considered. The cryptographic encryption algorithms used in cloud services were analyzed as well as comparative analysis of most popular up-to-date cloud services Wuala, DropBox and Google Drive was carried out. As the result of analysis, the advantages and the weakest places of each cloud services were defined. Besides that, in this work Google Drive work scheme and data protection in the cloud service were presented. The main disadvantage of cipher RC4-128, which is used in this cloud service, is identified. After this improved stream cipher based on RC4-128 has been developed. It contains additional byte transformations in the PRN formation algorithm, an additional PRN and a new incoming message encryption algorithm using the generated threads. As a result, these solutions provide the cryptographic security of the proposed stream cipher. Experimental study of improved stream cipher for cloud services was carried out. It was focused on data encryption speed research and statistical testing using the standardized NIST STS technique.

Keywords: cloud computing, cloud services, cloud security, cybersecurity, cryptography, stream cipher, algorithm, encryption, PRNG, RC4, NIST STS.

Introduction

In contemporary information and communication technology (ICT) world, cloud-based environments have been in active use for a long time: both on the Internet and across businesses. The potential for freely scalable technology allows not only to use direct-purpose information products, but also extending the administration and

maintenance of user-generated data, their processing and own funds usage in the field of cloud technologies [1].

Cloud technology topic is becoming wider. Contemporary scientific and practical conferences are devoted to further development and ways of building new infrastructure of the state, new technological solutions for ICT implementation. Cloud technologies are the basic infrastructure of the third generation, which allows to create powerful ICT with a new architecture and capabilities. According to the forecasts of the leading IT consulting companies in the world, the rapid improvement and spread of cloud computing will completely change the IT industry development in the coming years and will have a significant impact on other important spheres of human life.

The essence of "cloud" technologies [2] is to provide end users with remote dynamic access to computing resources, services and applications (including information and operating systems, server software, etc.) over the Internet or through a corporate network (Fig. 1 [3]). The tendency of hosting sphere development and necessity for people to use public resources was defined by the emergent need for new software and information digital services which could be managed from the inside but which would be more economical and efficient.

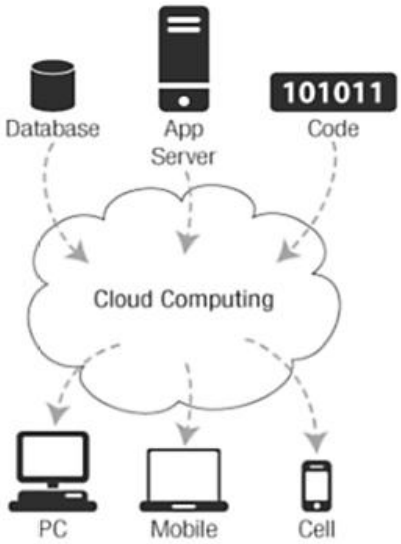

Fig. 1. Cloud computing scheme and concept

Using "cloud" technologies can not only reduce the cost of physical equipment, but also massively combine data with their subsequent protection, ability to work remotely with the enterprise information system and personalize "cloud" core for the needs of the company. But "cloud" technologies have several disadvantages. The main one is the threat to information security [4]. According to standards, described in work [1], *cloud security* means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to

provide integrity, confidentiality and availability in cloud services. In a highly competitive environment, companies are most afraid of: data leaks from the "cloud" provider network due to data interception, loss of control over data and applications, inability to destroy data, insider action by the provider or other "cloud" users. For protection it can be used data encryption or depersonalization. And not only the data stored with the provider, but also the channel of communication with it should be encrypted. Therefore, the development of really persistent data encryption algorithms as well as improving existing information security methods in cloud services are very relevant in our time and still actual in future during 5G-6G implementing.

The main purpose of the study is to provide cryptographic security in cloud services without reducing performance by improving stream cipher.

Up-to-date Cloud Services Review

Cloud services are the latest type of networking services that enable virtual media information to extend the hardware and software resources of a user's computer device. The cloud services emergence has become possible during development process of cloud computing technologies, which are implemented under the conditions of dynamic large-scale access to distributed external network resources. Providing such access as a separate service remains a type of cloud service [1-3].

Cloud services are usually provided on the Internet using modern Internet browsers. Cloud services utilize virtual machines that operate in large datacenters and replace physical personal computers and servers. The main difference from the usual use of software in cloud services is that the user can combine the internal resources of his computer device and the software resources provided to him as an online service. During this user has full access to managing his own data, but cannot control the operating system or software base through which this work is done.

2.1 DropBox Storage Service [5]

Login and registration. For registration and login, it is used secure communication channel (TLS). Registration can be done on the website or during client installation. During registration on the website the user has to enter his first and last name (arbitrary lines), email address and password. One email address can only be associated with one account. During registration, a minimum password length of at least six characters is imposed; a maximum limit is not set. In addition, no email address should be used as a password. During registration on the website DropBox provides a hint of the password quality, but accepts weak passwords. The registration process during client installation is slightly different: the client application does not have a password strength indicator and the user has to repeat the password. When entering a previously used address, a corresponding message is displayed. When first logged in through a client app, the user enters an email address and password. After passing the authentication, the security token is transmitted to the server and stored on the client side for further user authentication. DropBox does not send an activation message to

the email immediately after registration, it only happens after trying to get the first URL to share the file, so the user can use the new account as soon as fill in the registration form. In case of a failed login attempt, DropBox informs the user that one element of the login / password pair is incorrect but does not specify which one.

If a user has lost his password, Dropbox sends a message to the user's registered email. This email contains the URL of a secure web page for entering a new password. Dropbox prevents password hijacking by temporarily blocking your account after many unsuccessful attempts to sign in for a specified period of time. Dropbox has the ability to use two-factor authentication. This option can be enabled in profile settings. In can be used one-time access codes that can be received on a mobile phone. It is also possible to use barcodes using Time Based One Time Password mobile applications.

Secure communication channel (SCC). During the DropBox analysis, the principle of securing communication channel between the client and the server was considered.

SCC formation protocol – TLS.

Message authentication algorithm – AES_256_CBC (SHA1).

Key agreement algorithm – ECDHE_RSA (2048 bit).

Data storage security. DropBox uses AES-256 to encrypt data stored on servers. This data will not be encrypted on the client side, instead DropBox encrypts the data after booting on the server side using its own encryption key. Since DropBox encrypts data on the server, user can not be sure in data privacy.

Data encryption algorithm –AES-256.

Data encryption key possession – the key is owned by the provider.

2.2 Google Drive Storage Service [5,6]

Login and registration. A SCC is used to register and log in. New accounts can be created on a Google page. To use the service must have a Google account, which is the same for all services and email address tied to Gmail. During registration, the user must be sure to provide first and last name, gender, birth date, come up with a unique email address and enter password twice. Also need to enter information from the image. One email address can be associated with one account. To create a Google Account, you must select a password, which include at least 8 characters, but not more than 100 characters. In passwords can be used Latin letters (both large and small: A-Z, a-z), numbers (0-9) and punctuation marks. The password can consist of only one character's group. When creating a password, the system provides a password quality hint. Google also rejects common passwords. Thus, weak passwords are not accepted. Since the login is unique to all Google applications – no additional signup confirmation is required. If unsuccessful attempt to log in, Google notifies the user that one element of the pair login / password is not correct, but does not specify what kind of. If a user forgets his password, he gets two possible ways to set a new password:

- a secure page for resetting user's password, URL sent by mail;
- using a code that is sent to a mobile phone via a short message or can be communicated during a phone call.

Google prevents brute force passwords using mandatory requirements Input characters from the image after a series of failed login attempts in service. Google has the ability to use two-factor authentication, this option can be enabled in the profile settings. It is used one-time access codes that can be send on mobile phone.

SCC. During the analysis of Google Drive, the security principle for communication channel between client and server was considered.

SCC formation protocol – TLS.

Message authentication algorithm – RC4_128 (SHA1).

Key agreement algorithm – ECDHE_ECDSA (256 bit).

Data storage security. Google Drive does not use server-side data encryption.

2.3 Wuala Storage Service [7]

Login and registration. A SCC is used to register and log in. New accounts can only be created using the Wuala App. During registration a user must provide a unique name, email address and password. A single email address can be associated with multiple accounts. Only minimum lengths of at least six characters are imposed on the password, no maximum limit is set. Wuala provides hint about password quality during registration, but does not reject weak passwords. Wuala does not send an activation message to the email to confirm the fact of registration. In case of unsuccessful login attempt, Wuala informs the user that one or both of the elements of the login / password pair is incorrect but does not specify which one. Passwords are not stored on Wuala servers, so the ability to recover a lost password is not available.

Wuala provides optional password hint functionality. The password hint can be used for a single username or email address and will be sent to a registered email address. If there are multiple accounts registered with the same email address – multiple emails will be sent, one for each account that has a password hint. The password hint feature allows to collect information about already registered usernames and email addresses. There are no restrictions on the number of failed login attempts. Two-factor authentication is not currently implemented in Wuala.

SCC. The Wuala SCC uses its own client-server communication protocol rather than standardized and well-known SSL / TLS. According to Wuala press releases, integrity checks are being used to protect data during transmission, but no detailed documentation on mechanisms and protocols has been published. In conjunction with the convergent encryption schemes used by Wuala, the lack of encryption during transmission allows attackers to receive messages being transmitted and to attempt information-gathering attacks.

SCC formation protocol is absent.

Message authentication algorithm – AES_256 (SHA1)

Key agreement algorithm – DHE_RSA (2048 bit)

Data storage security. The idea behind Wuala encryption is to have an unreliable file system whose security is ensured by cryptographic methods. Used scheme is an implementation of directory tree structure for cryptographic file system called Cryptree.

Trust is based on a symmetrical root key that is obtained from a user's password. Wuala calculates the individual keys for each directory and the individual keys for

each file. They all are output through the root key. They can be provided to partners for the purpose of data exchange. Wuala uses converged encryption schemes. This means that key to encrypt the file is derived from its hash value.

The most *important properties of convergent encryption schemes* are:

1) Identical plaintexts are encrypted into identical crypto texts, regardless of user;

2) Server cannot decrypt the crypto texts without having a copy of the plaintext.

The first property ensures the implementation of encrypted data deduplication feature. The second property protects documents that are unique to the user, such as self-written works, unpublished technical reports, etc.

Converting encryption schemes, on the other hand, have important disadvantages, including the attacks possibility if the attacker has access to the server side. According to press releases, it is noted that Wuala uses AES-256 to encrypt metadata and stored information. The client signs each file with a pair of user keys, in order to identify files that were received from third parties. The signatures are created and verified using RSA-2048, while SHA-256 hash function is used to verify the integrity.

Data encryption algorithm – converged encryption scheme.

Data encryption key possession – the key is stored on the client side.

Table 1 presents what advantages and disadvantages of each studied cloud services [5-7]. So, unlike Wuala's service, Google Drive and DropBox have two-factor authentication, password-attack protection, password recovery mechanism and transfer data by TLS 1.1 protocol (SCC formation protocol).

Table 1. Comparative analysis of modern cloud services

Cloud service	**Protection against brute force attacks**	**Two-factor authentication**	**Pass recovery mechanism**	**SCC formation protocol**	**Message authentication algorithm**	**Key agreement algorithm**	**Data encryption algorithm**
DropBox	Temporary lock	Password and OTP	Present	TLS 1.1	AES_256_CBC (SHA1)	ECDHE_RSA (2048 bit)	AES-256
Google Drive	Using characters from the image	Password and OTP	Present	TLS 1.1	RC4_128 (SHA1)	ECDHE_ECDSA (256 bit)	-
Wuala	Absent	Absent	Absent	Absent	AES_256 (SHA1)	DHE_RSA (2048 bit)	Converged encryption scheme

One of the major drawbacks of each service is that message authentication uses the SHA1 algorithm, which is considered as outdated and not resistant to hacking. In Google Drive for messages authentication along with the SHA1 algorithm uses an algorithm RC4 that is also a disadvantage of service because it was proven that the modern attacks on the RC4 allow to break it for a few days or even hours. Another drawback of Google Drive is that it does not implement server-side data encryption. Wuala uses the Diffie-Hellman protocol for key agreement, while Google Drive and DropBox use the Diffie-Hellman protocol on elliptic curves.

Table 2 shows the analysis of the basic encryption algorithms used in cloud services. This also was given from previous review part [5-7].

Table 2. Analysis of cryptographic algorithms used in cloud services

Encryption algorithm	Cloud services	Type	Advantages	Disadvantages
AES	DropBox, Wuala	Block cipher	Provides high practical security, effective for implementation on 32-bit platforms, has a number of hardware accelerators	Known theoretical attacks with complexity less than a complete search; can not fully use the capabilities of 64-bit platforms; relative obsolescence
RC4	Google Drive	Stream cipher	High speed, variable key size	Vulnerable when using non-random or related keys, one key stream is used twice.
SHA1	DropBox, Wuala, Google Drive	Block cipher	Fast enough, easy to implement	Does not guarantee sufficient protection against attacks

Next Section of the paper consists on improvement of cryptographic security of Google Drive that is most effective among analyzed cloud services; it based on stream cipher but has some vulnerability (Table 2).

This is very important issue because possible types of security challenges for cloud computing services include compromises to the confidentiality and integrity of data in transit to and from a cloud provider and at rest [1,8].

Improving Stream Cipher for Cloud Services

3.1 RC4 Stream Cipher Description

Google Drive is data store owned by Google Inc. that allows users to store their data on servers in the cloud and share it with other users on the Internet.

During the analysis of Google Drive, the principle of securing communication channel between the client and the server was considered in Section 2. Let's take a closer look at the RC4-128 message encryption algorithm [9]. RC4 is streaming cipher developed by Ron Rivest in 1987, when he worked for the US company RSA Security. Has become a common algorithm used in such popular protocols as TLS (to secure internet traffic) and WEP (for wireless network security). Among others, it stands out for its speed and ease of software implementation, but the PC4 has flaws that indicate its inappropriate use in the latest systems. RC4-128 uses a sequence of numbers from 0 to 127 in the array *S*, which changes when algorithm works (Fig. 2).

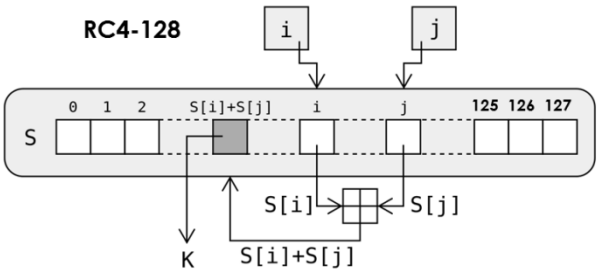

Fig. 2. Scheme of RC4-128 stream cipher realization

RC4-128 consists of following processes: Key Scheduling Algorithm (KSA), Pseudo-random Number Generation (PRNG) and Data Encryption. These processes are described by Pseudo-code 1. Besides that, RC4 is value part of security system in BitTorrent, Skype, Opera, Kerberos, PDF etc.

Pseudo-code 1:

1. .KSA to set the initial value of the array *S*:
   - 1.1. KSA stars work with S initialization such as *S*[*i*]=*i*, for $i = \overline{0,127}$.
   - 1.2. The secret key is given by a set of numbers, which are placed in a key array *K*, that also contains128 elements. Usually, a short sequence of numbers is selected, which is then repeated until *K* is filled.
   - 1.3. The key array is used to convert S by the following scheme:
     - 1.3.1. *j*=0;
     - 1.3.2. For $i = \overline{0,127}$ the following steps are performed:
       - 1.3.2.1. *j*=(*j*+ *S*[*i*] + *K*[*i*])mod128;
       - 1.3.2.2. *buf*=*S*[*i*]; *S*[*i*]=*S*[*j*]; *S*[*j*]= *buf*.
2. PRNG algorithm for encryption:
   - 2.1. A byte array *k* of PRN is generated, selecting random elements of the *S* array for the next sample:
     - 2.1.1. *i* = 0; j = 0;
     - 2.1.2. The following algorithm is used to generate each byte of a random stream:
       - 2.1.2.1. *i* = (*i*+1)mod128;
       - 2.1.2.2. *j* = (*j*+*S*[*i*])mod128;
       - 2.1.2.3. *buf*=*S*[i]; *S*[*i*]=*S*[*j*]; *S*[*j*]= *buf*.
       - 2.1.2.4. *t* = (*S*[*i*] + *S*[*j*])mod128;
       - 2.1.2.5. *k* = *S*[*t*]
3. Data Encryption:
   - 3.1. *X*-plain text; *Y*-ciphertext; $Y_i = X_i \oplus k$.

The Fast Software Encryption Cryptographic Conference took place in Singapore in 2013, the main event being the speech of American Professor Dan Bernstein, who introduced the method of bypassing TLS (Transport Layer Security) and SSL (Secure Sockets Layer) protocols if they use RC4 encryption algorithm [10].

Successful attack on the cipher can be carried out due to insufficient randomness of the bit stream to which the message is transmitted. If chase a large number of network packets through this stream, it can be detected enough repetitive patterns to get the original content of the message. Successful attacks require the capture of large amounts of encrypted traffic. The researcher reported that he managed to bypass TLS protection in 32 hours, but hackers can apply various techniques to optimize and accelerate the RC4 hacking process. Apparently, this encryption algorithm is not crypto resistant (secure) and requires improvement [11].

3.2 Proposed Improving of RC4 Stream Cipher

Therefore, improved stream cipher called ISC2k19 was developed, which eliminates the disadvantages of RC4 by changing the PRNG algorithm to substitution table implementation (S-box) and the use of constants, generation of additional PRNG flow and data encryption algorithm changing, which allows to increase the cryptographic security [12] of the algorithm.

ISC2k19 uses a sequence of numbers from 0 to 255 in the array *S*, which changes during algorithm works. ISC2k19 consists of four following processes (described by Pseudo-code 2):

Pseudo-code 2:

1. KSA to set the initial value of the array *S*:
   1.1. KSA stars work with *S* initialization such as $S[i]=i$, for $i = \overline{0,127}$.
   1.2. The secret key is given by a set of numbers that are placed in the key array *K*, which also contains 128 elements. Usually, a short sequence of numbers is selected, which is then repeated until *K* is filled.
   1.3. The key array is used to convert *S* by the following scheme:
      1.3.1. $j=0$;
      1.3.2. For $i = \overline{0,127}$ the following steps are performed:
         1.3.2.1. $j=(j+ S[i] + K[i])\bmod 128$;
         1.3.2.2. Then $S[i]$ and $S[j]$ are modified using a tables of substitutions (S-box, Table 3) and constants (Const, Table 4);
         1.3.2.3. $S[j]= Sbox\,(S[j]+Const[i])$; $S[i]= Sbox(S[i])$.
         1.3.2.4. $buf=S[i]$; $S[i]= S[j]$; $S[j]= buf$.
2. PRNG algorithm for randomly selecting array elements and changing array *S*, for $S[i]$, where $i = \overline{0,127}$.
   2.1. A byte array of PRN is generated by selecting random elements of array *S* for the next sample:
      2.1.1. $i = 0$; $j = 0$;
      2.1.2. The following algorithm is used to generate each byte of a random stream:
         2.1.2.1. $i = (i+1)\bmod 128$;
         2.1.2.2. $j = (j+S[i])\bmod 128$;
            2.1.2.3. Then $S[i]$ and $S[j]$ are modified using a tables of substitutions (S-box, Table 3) and constants (Const, Table 4);
            2.1.2.4. $S[j]= Sbox\,(S[j]+Const[i])$; $S[i]= Sbox(S[i])$
            2.1.2.5. $buf=S[i]$; $S[i]=S[j]$; $S[j]= buf$.
            2.1.2.6. $t = (S[i] + S[j])\bmod 128$;
            2.1.2.7. $k = S[t]$.
3. The algorithm for generating an additional stream of PRN for randomly selecting array elements and changing array *S*, $S[i]$, where $i = \overline{128,255}$.

3.1. Bytes r of PRN of key are generated by selecting random array S elements.

3.1.1. i= 128, j=0.

3.1.2. j=(j+1)mod128.

3.1.3. $S[m] = S[i\text{-}1] \oplus (S[i\text{-}1] <<< j)$.

3.1.4. $r = S[m]$.

4. Data encryption:

4.1. X- plain text; Y-ciphertext; $Y_i = \begin{cases} X_i \oplus k, i\text{mod}2 = 0; \\ X_i <<< r, i\text{mod}2 = 1. \end{cases}$

Both Table 3 and Table 4 are used in PRNG algorithm forming process of ISC2k19 stream cipher for security improving.

Table 3. Substitutions table (S-box) of ISC2k19 stream cipher

\	0	1	2	3	4	5	6	7	8	**9**	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	**d4**	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Table 4. Table of constants (Const) of ISC2k19 stream cipher

Index	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
Constant	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16
Index	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**
Constant	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
Index	**32**	**33**	**34**	**35**	**36**	**37**	**38**	**39**	**40**	**41**	**42**	**43**	**44**	**45**	**46**	**47**
Constant	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08

Index	**48**	**49**	**50**	**51**	**52**	**53**	**54**	**55**	**56**	**57**	**58**	**59**	**60**	**61**	**62**	**63**
Constant	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
Index	**64**	**65**	**66**	**67**	**68**	**69**	**70**	**71**	**72**	**73**	**74**	**75**	**76**	**77**	**78**	**79**
Constant	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
Index	**80**	**81**	**82**	**83**	**84**	**85**	**86**	**87**	**88**	**89**	**90**	**91**	**92**	**93**	**94**	**95**
Constant	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
Index	**96**	**97**	**98**	**99**	**100**	**101**	**102**	**103**	**104**	**105**	**106**	**107**	**108**	**109**	**110**	**111**
Constant	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
Index	**112**	**113**	**114**	**115**	**116**	**117**	**118**	**119**	**120**	**121**	**122**	**123**	**124**	**125**	**126**	**127**
Constant	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75

Next Section of this work contains experimental technique as well as study of RC4 and improved stream cipher (ISC2k19).

Experimental Study of Stream Ciphers

4.1 Experimental Research Technique

An experimental study conducted to confirm or refute the hypothesis. To obtain the maximum result, it is necessary to clearly describe the study methodology. The conclusions of the theory, that would be experimentally studied should include only observable quantities. If it is difficult to predict the result theoretically, it is advisable to use statistical results. These experiments are based on traditional standards of research study in cryptography [13-15] and particularly in stream cipher security analysis [16-18]. To perform each experiment study, it is necessary:

1. Determine the experimental purpose;
2. Set a target task;
3. Select the research object;
4. Identify input and output data;
5. Create a program of experimental work;
6. Determine the methods and techniques of intervention in the research object;
7. Develop techniques for recording the progress and results of the experiment;
8. Prepare instruments, devices, applications, etc.

According to the hypothesis, the qualitative nature of the expected results is predetermined: this will ensure a quick and correct evaluation of them, instantly alert with unexpected results, and help to avoid false conclusions.

4.2 Experimental Study of Ciphers Speed (Experiment №1)

The purpose of this experiment is study the speed characteristics of RC4 and improved stream cipher ISC2k19. To achieve mentioned purpose the following *tasks* should be performed:

1. Estimation the speed of 100KB data cryptographic transformation by software application based on both stream ciphers;
2. Estimation the speed of 1MB data cryptographic transformation by software application based on both stream ciphers;
3. Estimation the speed of 10 MB data cryptographic transformation by software application based on both stream ciphers;
4. Estimation the speed of 100 MB data cryptographic transformation by software application based on both stream ciphers.

Research object: the process of data cryptographic transformation.
Input data: encryption file, key stream.
Output data: encryption/decryption speed.

The experiment is performed manually with the help of the developed software application; the results are recorded in the Table 6. To confirm the achievement of this purpose, a comparative speed test of the encryption and decryption was carried out (between software-implemented cipher RC4-128 and developed ISC2K19 cipher). Testing was performed on four different computers; the characteristics of their hardware are given in Table 5.

Table 5. The characteristics and CPUs of the machines being tested

№	Processor
1	Intel Pentium CPU G4400 3.30GHz
2	Intel Pentium CPU G4520 3.6GHz
3	Intel Core CPU i3-6100T 3.2GHz
4	Intel Core CPU i7-5775R 3.3GHz

Testing was carried out for four selected files of different sizes (Table 6).

Table 6. Average speed test results for two studied ciphers

Stream Cipher	Processor			
	1, MB/s	**2, MB/s**	**3, MB/s**	**4, MB/s**
RC4-128	24,1	23,6	22,7	25,8
ISC2K19	20,3	20,2	19,5	20,9

The speed of ISC2K19 algorithm averaged was 20,2 MB/s, while the RC4-128 speed is 24,05 MB/s. Therefore, the improved stream cipher ISC2K19 showed worse results than RC4-128 during speed tests by 14.8%. But since the difference in time between RC4-128 and ISC2K19 data encryption is negligible, the speed of ISC2K19 is not a major disadvantage (security is priority parameter).

4.3 Experimental Study of Ciphers Statistical Security (Experiment №2)

The purpose of this experiment is study the statistical characteristics of cryptographic security of RC4 and improved stream cipher ISC2k19. To achieve mentioned purpose the evaluation the statistical characteristics of both stream ciphers using the NIST STS technique.

Research object: data encryption process.

Input data: encrypted files by size 100 KB, 1MB, 10MB, 100MB.

Output data: test coefficients.

The experiment is performed by a console version of the NIST STS [19]. In accordance to [20-21] the most modern analytical attacks are statistical; during cryptanalysis, a large number of encryptions are performed to obtain a key, and round key variants are formed based on ciphertexts. When processing a sufficiently large sample of ciphertexts formed on a single key, the correct value of key bits is more common that the other variants. Obviously, the probability of finding the right pair, which gives a specific value of the key, depends on the statistical properties of the cipher. To increase the complexity of cryptanalysis, the properties of cryptograms must be close to random sequences. Therefore, a necessary (but not sufficient) condition for cipher security to analytic attacks is to provide good statistical properties of the output sequence (ciphertexts).

To test the statistical characteristics of the developed cryptoalgorithm it was tested in accordance with the NIST STS technique [19]. Software implementation of the algorithm is subjected to statistical testing using the NIST STS. The following parameters were selected for testing:

1. The length of the tested sequence $n=10^6$ bit;
2. The number of tested sequences $m=100$;
3. Significance level $\alpha=0,01$.

Thus, the sample size under test was $N = 100 \times 10^6$ bit; number of tests q for different lengths $q = 188$. Thus, the statistical portrait of the generator contains 18800 values of P probability.

In the ideal case, with specified parameters, only one sequence of one hundred can be discarded during testing, so the pass speed of each test should be 99%. But this restriction is too strict, so a rule based on the rj confidence interval applies. The lower bound in this case is the value $P_{\min} = 0,96015$. From this viewpoint, the results of testing cryptographic algorithm and the key extension algorithm were analyzed.

Table 7. Averaged NIST test results for two studied stream ciphers

Generator	Number of tests, which have been tested more than 99% sequence	Number of tests, which have been tested more than 96% sequence	The number of tests in which values P>0,01	The number of tests in which values P>0,001
RC4-128	125 (66,49%)	187 (99,46%)	147 (78,19%)	187 (99,46%)
ISC2K19	134 (71,28%)	188 (100%)	161 (85,63%)	188 (100%)

Analyzing the results, it can be conclude that the software implementation of the improved stream cipher passed complex control according to the NIST STS technique and showed better results than RC4-128 on 4.7%.

Conclusions

In the paper up-to-date cloud services Wuala, DropBox and Google Drive was analyzed, this made it possible to understand the schemes of their work, to determine what security methods and algorithms are used for data transmission as well as the main advantages and disadvantages of cloud services were emphases. Besides, the analysis of cryptographic methods and systems used in cloud services were carried out. This made it possible to understand what are the disadvantages of encryption algorithms and how to get rid of them.

An improved stream cipher ISC2k19 based on RC4-128 (used in TLS, SSL, SSH, WEP, BitTorrent, Skype, Opera, Kerberos, PDF) was developed to provide cryptographic security in cloud services without reducing performance (this improvement is directed on the most effective cloud service Google Drive). This cipher contains additional byte transformations in the algorithm of PRN formation. An additional PRN is also generated.

Experimentally the speed of ISC2k19 realization was compared with RC4-128 and the speed of ISC2K19 showed worse results than RC4-128 during speed tests by 14.8%. But since the difference in time between RC4-128 and ISC2K19 data encryption is negligible, the speed of ISC2K19 is not a major disadvantage. Also was performed an experimental study of security using the NIST STS: ISC2K19 passed complex control by NIST STS and showed better results than RC4-128 on 4.7%.

The future research study can be related with ISC2K19 security analysis and quantitative assessment of its security against various cryptanalytic attacks [22].

References

1. *NIST Cloud Computing Standards Roadmap*, National Institute of Standards and Technology Special Publication 500-291 V2, 108 p., 2013.
2. H. Susanto, M.N. Almunawar and C.C. Kang, "Toward Cloud Computing Evolution: Efficiency vs Trendy vs Security", *Computer Science Journal & Social Science Research Network*, September 2012, pp. 1-12.
3. ST Louis Cloud Computing – Cloud Hosting – Virtual Servers, Available online, URL: http://www.accessus.net/business-services/cloud-computing/
4. Z. Hu, S. Gnatyuk, O. Koval, V. Gnatyuk, S. Bondarovets, "Anomaly Detection System in Secure Cloud Computing Environment", *International Journal of Computer Network and Information Security (IJCNIS)*, vol. 9, no. 4, pp. 10-21, 2017.
5. C. Chu, W. Zhu, J. Han, J. K. Liu, J. Xu and J. Zhou, "Security Concerns in Popular Cloud Storage Services", in *IEEE Pervasive Computing*, vol. 12, no. 4, pp. 50-57, Oct.-Dec. 2013.
6. V.J. Raymond and E. Sushmitha, "Google drive based secured anti-theft android application", *2017 International Conference on IoT and Application (ICIOT)*, pp. 1-8, 2017.

7. Information Security. How does Wuala store symmetric key? Available online, URL: https://security.stackexchange.com/questions/37247/how-does-wuala-store-symmetric-key
8. Z. Xiao and Y. Xiao, "Security and privacy in cloud computing", *IEEE Commun. Surveys Tuts.*, vol. 15, no. 2, pp. 843-859, 2nd Quart., 2013.
9. G. Paul and S. Maitra, "RC4 Stream Cipher and its Variants", Boca Raton, FL, USA: CRC Press, 2011.
10. D. Bernstein, Failures of secret-key cryptography, Available online, URL: https://www.iacr.org/workshops/fse2013/slides/Slides07.pdf
11. B. Subhadeep; I. Takanori, Cryptanalysis of the Full Spritz Stream Cipher. *Lecture Notes in Computer Science,* Springer Berlin Heidelberg. pp. 63-77, 2016.
12. Z. Hu, S. Gnatyuk, M. Kovtun, N. Seilova, "Method of searching birationally equivalent Edwards curves over binary fields," *Advances in Intelligent Systems and Computing*, vol. 754, pp. 309-319, 2019.
13. S. Gnatyuk, V. Kinzeryavyy, M. Iavich et al, "High-Performance Reliable Block Encryption Algorithms Secured against Linear and Differential Cryptanalytic Attacks," *CEUR Workshop Proceedings,* vol. 2104, pp. 657-668, 2018.
14. S. Das, J. U. Zaman, R. Ghosh, "Generation of AES S-boxes with various modulus and additive constant polynomials and testing their randomization", *Proc. Technol.*, vol. 10, pp. 957-962, 2013.
15. Gnatyuk S., Akhmetov B., Kozlovskyi V. et al, "New Secure Block Cipher for Critical Applications: Design, Implementation, Speed and Security Analysis", *Advances in Intelligent Systems and Computing,* vol. 1126, pp. 93-104, 2020.
16. O. Kuznetsov, M. Lutsenko and D. Ivanenko, "Strumok stream cipher: Specification and basic properties", *2016 3rd International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T),* Kharkiv, pp. 59-62, 2016.
17. I. Gorbenko, A. Kuznetsov, M. Lutsenko and D. Ivanenko, "The research of modern stream ciphers", *2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T),* Kharkiv, pp. 207-210, 2017.
18. A. Kuznetsov, V. Frolenko, E. Eremin and O. Zavgorodnia, "Research of cross-platform stream symmetric ciphers implementation", *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT),* Kyiv, Ukraine, pp. 300-305, 2018.
19. *A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications.* NIST Special Publication 800-22, May 15, 2001, 164 p.
20. I. Gorbenko, O. Kuznetsov, Y. Gorbenko, A. Alekseychuk, V. Tymchenko, "Strumok keystream generator", *2018 IEEE 9th International Conference on Dependable Systems Services and Technologies (DESSERT),* Kyiv Ukraine, pp. 294-299, 2018.
21. O. Nariezhnii, E. Eremin, V. Frolenko, K. Chernov, T. Kuznetsova and I. Chepurko, "Research of Statistical Properties of Stream Symmetric Ciphers", *2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T),* Kharkiv, Ukraine, pp. 696-700, 2018.
22. B. Akhmetov, S. Gnatyuk, V. Kinzeryavyy, Kh.Yubuzova, Studies on practical cryptographic security analysis for block ciphers with random substitutions, *International Journal of Computing,* vol. 19, issue 2, pp. 298-308.