ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

А.БАЙТҰРСЫНОВ АТЫНДАҒЫ ҚОСТАНАЙ ӨҢІРЛІК УНИВЕРСИТЕТІ

Center of Excellence NIS Nazarbayev Intellectual Schools

ҚОСТАНАЙ ОБЛЫСЫ ӘКІМДІГІ МӘДЕНИЕТ БАСҚАРМАСЫНЫҢ "ЫБЫРАЙ АЛТЫНСАРИННІҢ ҚОСТАНАЙ ОБЛЫСТЫҚ МЕМОРИАЛДЫҚ МҰРАЖАЙЫ" КОММУНАЛДЫҚ МЕМЛЕКЕТТІК МЕКЕМЕСІ

КОММУНАЛЬНОЕ ГОСУДАРСТВЕННОЕ УЧРЕЖДЕНИЕ "КОСТАНАЙСКИЙ ОБЛАСТНОЙ МЕМОРИАЛЬНЫЙ МУЗЕЙ ИБРАЯ АЛТЫНСАРИНА" УПРАВЛЕНИЯ КУЛЬТУРЫ АКИМАТА КОСТАНАЙСКОЙ ОБЛАСТИ

АЛТЫНСАРИН ОҚУЛАРЫ

«ИННОВАЦИЯ, БІЛІМ, ТӘЖІРИБЕ-БІЛІМ БЕРУ ЖОЛЫНЫҢ ВЕКТОРЛАРЫ»

ХАЛЫҚАРАЛЫҚ ҒЫЛЫМИ-ПРАКТИКАЛЫҚ КОНФЕРЕНЦИЯСЫ

МАТЕРИАЛДАРЫ

I КІТАП

АЛТЫНСАРИНСКИЕ ЧТЕНИЯ

МАТЕРИАЛЫ

МЕЖДУНАРОДНОЙ НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ

«ИННОВАЦИИ, ЗНАНИЯ, ОПЫТ – ВЕКТОРЫ ОБРАЗОВАТЕЛЬНЫХ ТРЕКОВ»

I КНИГА

Қостанай, 2023

УДК 37.02
ББК 74.00
И 63

«Инновация, білім, тәжірибе-білім беру жолының векторлары»: 2023 жылдың 17 ақпандағы Халықаралық ғылыми-тәжірибелік конференция материалдары. I Кітап. – Қостанай: **И 63** А.Байтұрсынов атындағы Қостанай өңірлік университеті, 2023. – 1081 б. = «Инновации, знания, опыт – векторы образовательных треков»: Материалы международной научно-практической конференции, 17 февраля 2023 года. I Книга. – Костанай: Костанайский региональный университет имени А.Байтурсынова, 2023. – 1081 с.

ISBN 978-601-356-244-5

Жинаққа «Инновация, білім, тәжірибе-білім беру жолының векторлары» атты Алтысарин оқулары халықаралық ғылыми-практикалық конференция материалдары енгізілген.

Талқыланатын мәселелердің алуан түрлілігі мен кеңдігі мақала авторларына заманауи білім беруді жаңғырту мен дамытудың, осы үдерісте қазақ ағартушыларының педагогикалық мұрасын пайдаланудың жолдарын, мұғалімдерді даярлаудың тиімді технологиялары мен форматтарын әзірлеу мен енгізу мәселелерін, ақпараттық қоғамдағы білім беру кеңістігінің ерекшеліктерін айқындауға, сондай-ақ педагогтердің инновациялық қызметінің тәжірибесін жинақтауға, педагогикалық үдеріс субъектілерін психологиялық-педагогикалық қолдауға мүмкіндік берді.

Бұл жинақтың материалдары ғалымдарға, жоғары оқу орындары мен колледж оқытушыларына, мектеп мұғалімдері мен мектепке дейінгі тәрбиешілерге, педагог-психологтарға, магистранттар мен студенттерге қызықты болуы мүмкін.

В сборнике содержатся материалы Международной научно-практической конференции Алтынсаринские чтения «Инновации, знания, опыт – векторы образовательных треков». Многообразие и широта обсуждаемых проблем позволили авторам статей определить векторы модернизации и развития современного образования, использования в данном процессе педагогического наследия казахских просветителей, вопросов разработки и внедрения эффективных технологий и форматов подготовки учителей, специфики образовательного пространства в информационном обществе, а также обобщения опыта инновационной деятельности педагогов, психолого-педагогической поддержки субъектов педагогического процесса.

Материалы данного сборника могут быть интересны ученым, преподавателям вузов и колледжей, учителям школ и воспитателям дошкольных учреждений, педагогам-психологам, магистрантам и студентам.

ISBN 978-601-356-244-5

9 786013 562445

УДК 37.02
ББК 74.00

УДК 371.3

TEACHING CRYPTANALYSIS OF CLASSIC ENCRYPTION METHODS USING MODERN TOOLS

Qozoqova To'xtajon Qaxramon qizi
Assistant,Tashkent University of Information
Technologies named after Muhammad al–Khwarizmi
Tashkent, Uzbekistan
E–mail: toxtajonqozoqova31@gmail.com

Аңдатпа

Бұл мақалада криптоталдау процесі заманауи бағдарламалық құралдарды қолдану арқылы жүзеге асырылды және нәтижелер алынды, және біз осы Cryptool бағдарламасын пайдаланып талдауға кететін уақыттың айтарлықтай қысқарғанын көреміз. Онлайн–бағдарламадан аталған классикалық шифрлау алгоритмдерін пайдалану мүмкіндігі жаңа студенттер үшін өте ыңғайлы.

Түйін сөздер*: Cryptool Цезарь, Атбаш, Полибий, Вигенер, Дөрекі күш шабуылы*

Аннотация

В данной статье был проведен процесс криптоанализа с использованием современных программных средств и получены результаты, и мы видим, что время, необходимое для анализа с использованием данной программы Cryptool значительно сокращается. Возможность использования упомянутых классических алгоритмов шифрования из программы онлайн очень удобна для новых учеников.

Ключевые слова: *Cryptool , Цезарь, Атбаш, Полибий, Вигенер, Атака грубой силы*

Abstract

In this article the process of cryptanalysis using modern software tools was carried out and the results were obtained, and we see that the time required for analysis using this Cryptool program is significantly reduced. The possibility of using the mentioned classic encryption algorithms from the online program is very convenient for new students.

Key words: *Cryptool, Caesar, Atbash, Polybius, Vigenere, Brute Force Attack*

Caesar's encryption algorithm. Julius Caesar uses the following encryption algorithm in his letters to ensure mission confidentiality when sending confidential tasks by letter. Instead of the uppercase and lowercase Latin letters involved in the letter, he writes a letter that comes after the letter K in the alphabet (he thinks that the letter a comes after the letter z in the alphabet). The encryption can be expressed using modular arithmetic by first converting the letters into numbers according to the scheme A = 0, B = 1,..., Z = 25. Encryption of a letter can be mathematically described by n shifts.

$$E_x(x) = (x + n)mod26$$

For example, when K = 3: Message: abcdefghijklmnopqrstuvwxyz. Password: defghijklmnopqrstuvwxyzabc. The following formula is used for decryption, which is the reverse of encryption

$$D_x(x) = (x - n)mod26$$

In cryptanalysis of the Caesar cipher, the following two situations can be considered:

1) The parser knows (or guesses) that some simple replacement cipher is being used, but it is not a Caesar cipher;

2) the parser knows that he is using a Caesar cipher, but does not know the shift value.

In the first case, the cipher can be cracked using techniques such as frequency analysis or pattern words, as in the case of a simple substitution cipher. The analyst can quickly detect a pattern in the solution and conclude that the Caesar cipher is the particular algorithm in use.We use Cryptool software to perform ryptanalysis in Caesar. You download the program from https://www.cryptool.org/en/ct2/downloads and run it. The main window of the program is shown in Figure 1.

Figure 1. Cryptool main window

The templates section of Cryptool has cryptanalysis templates, and the result is obtained by entering the analysis sequence into this ready template or empty window. The Cryptanalysis section is divided into classic and modern sections. In Figure 2 below, Caesar's encryption algorithm has been analyzed using the frequency analysis method.

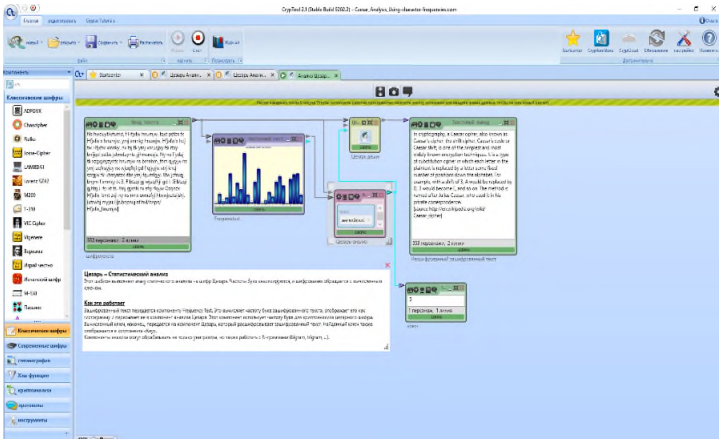
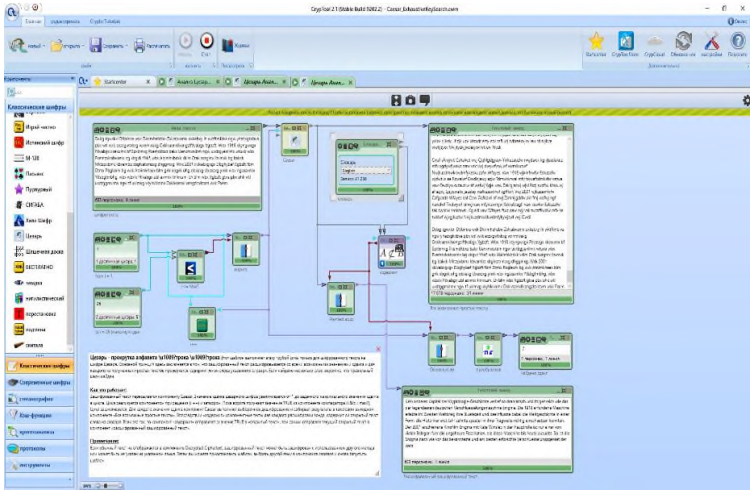


Figure 2. Caesar cipher frequency analysis method

Figure 3. Trying the Caesar cipher



We also use brute force analysis for the Caesar cipher.Figure 3 shows the result of brute force analysis. The code is entered in the part marked in the picture.

Atbash encryption algorithm. Atbash is an ancient encryption system created in the Middle East. It was originally used in Hebrew; some historians and cryptographers believe there are examples in the Bible. The name «Atbash» comes from the first Hebrew letter Aleph and the last letter Taf. The atbash cipher is a

simple permutation cipher based on rearranging all the letters of the alphabet so that the result is reversed. Atbash is also a substitute for a password. Since each letter corresponds to another, it provides very little security. The first letter is replaced by the last letter, the second letter by the penultimate letter, and so on. The finished cipher looks like this:

Massage: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher: ZYXWVUTSRQPONMLKJIHGFEDCBA

An example of plaintext encrypted text using Atbash:

Massage: MEETMEATONE
Cipher: NVVGNVZGLMV

As you can see and as mentioned above, the atbash cipher provides no security once the encryption method is found. https://www.cryptool.org/en/cto/atbash provides atbash encryption at the link below. Figure 4 shows an example of the atbash cipher.

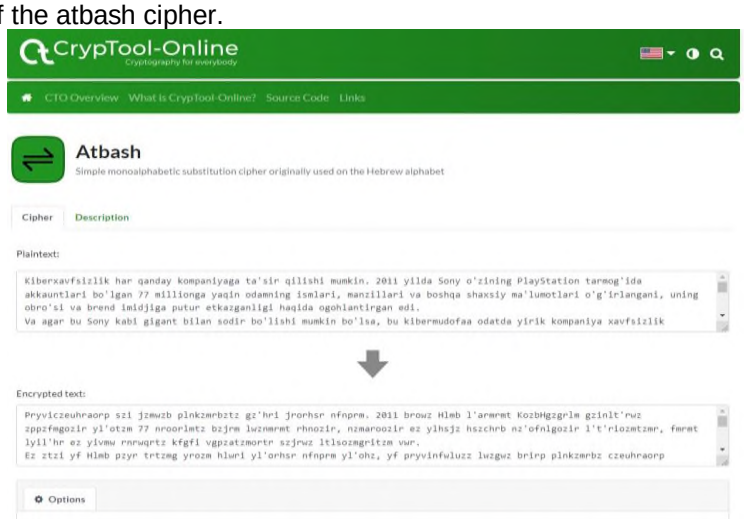
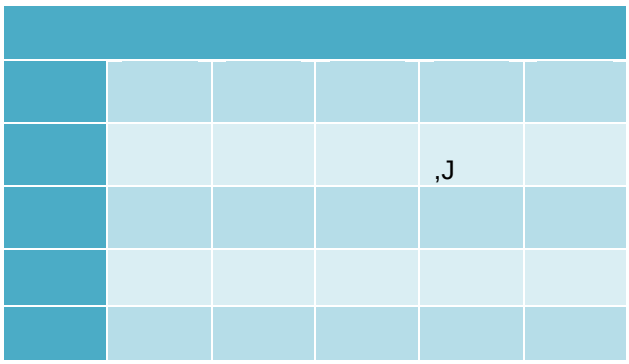


Figure 4. Atbashda password online result

Polybius encryption algorithm. A Polybius square is a table that allows someone to convert letters into numbers. This table can be randomized and passed to the recipient to make encryption a little harder. To fit the 26 letters of the alphabet into the 25 cells created in the table, the letters "i" and "j" are usually combined into one cell. Originally there was no such problem because the ancient Greek alphabet had 24 letters. The size of the square changes depending on the type of the alphabet (Table 1).

Table 1



Encryption is based on this table, for example, we encrypt the word «cybersecurity» based on the Polybius table.

Plain text = cybersecurity

Cipher text =25241215425311512143245531 2425

Encryption is done online at https://cryptii.com/pipes/polybius–square, and decryption can be done at the same address. Figure 5 shows the process.

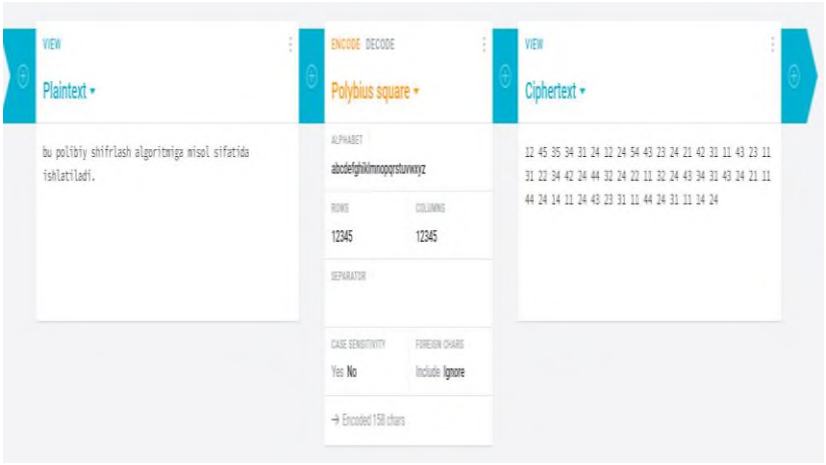


Figure 5: Process of online encryption and decryption of the Polybius cipher

Vigenere encryption algorithm. Vigenere encryption weakens the frequency characteristics of the appearance of characters in the text, but some features of the appearance of characters in the text are preserved. The main disadvantage of the Wiener cipher is that its key is repeated. Thus, a simple cryptanalysis of the cipher can be constructed in two steps:

1. Finding the key length. The distribution of frequencies in the ciphertext can be analyzed in different ways. That is, obtain a text containing every second letter of the ciphertext, then every third letter, and so on. As soon as the frequency distribution of the letters differs significantly from the uniformity (e.g. by entropy), we can talk about the length of the key found.

2. Cryptanalysis. l A set of Caesar ciphers (where l is the length of the found key), which are easily cracked individually. The Friedman and Kasiski tests help determine the length of the key.

Table 2

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

This component uses the output to find the secret key. Key sizes from one to twenty are tested. Normal text and the best candidates are displayed in the leaderboard. You can also use this template to create plaintext by selecting keys automatically selected by the Vigenere encryption algorithm. To do this you need to set the «auto–key» on the analyzer, the process is shown in Figure 6.

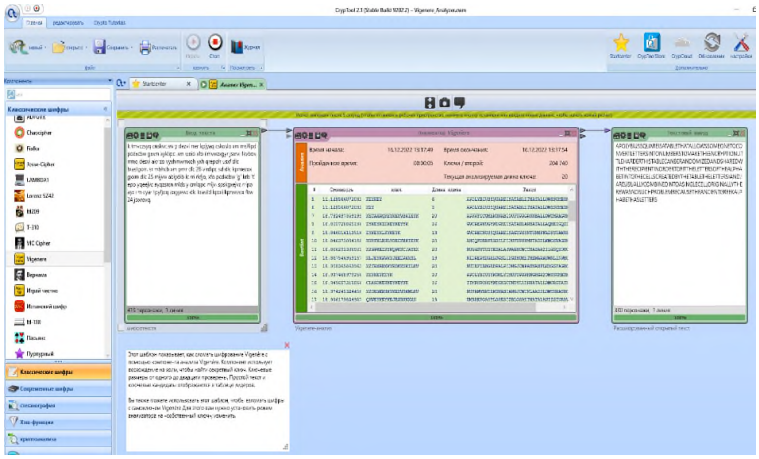


Figure 6. Process of cryptanalysis of the Wegener's encryption algorithm

In conclusion, we can say that the time required for cryptanalysis in the software tools of modern information technology has proven to be more advanced and less time–consuming than the traditional method of analysis. The implementation of these software tools in the educational process is found to be effective. This article is given as a practical work to the student as an assignment on cryptanalysis, and we get new results from them

References:

1. Aakanksha Sharma «Comparative Study of Symmetric Cryptography Algorithm» dissertation work. Udaipur 2014
2. Linda Rosencrance «Cryptoanalsys» search security 2021 y
3. Joan Daemen, Lars Knudsen, Vincent Rijmen (January 1997). The Block Cipher Square (PDF). 4th International Workshop on Fast Software Encryption (FSE '97), Volume 1267 of Lecture Notes in Computer Science. Haifa: Springer–Verlag
4. Farzaneh Abed, Eik List, Stefan Lucks, and Jakob Wenzel Bauhaus Cryptanalysis of the Speck Family of Block Ciphers Revision From October 9, 2013Universität Weimar, Germany
5. Robert Brummayer and Armin Biere «Boolector: An Efficient SMT Solver for Bit–Vectors and Arrays» Institute for Formal Models and Verification Johannes Kepler University Linz
6. Chistofer Smitson «Modern Cryptoanalsys» Unireversity of Tulsa 2020
7. To'xtajon Qozoqova «Cryptanalysis methods of symmetric block ciphers» master's thesis. Toshkent 2022
8. https://www.cryptool.org/en/cto/atbash
9. https://cryptii.com/pipes/polybius–square
10. https://en.wikipedia.org/wiki/Cryptanalysis
11. https://en.wikipedia.org/wiki/Linear_cryptanalysis

УДК 373.51

СОВРЕМЕННАЯ ЦИФРОВАЯ СРЕДА КАК ФАКТОР ПОВЫШЕНИЯ УРОВНЯ МАТЕМАТИЧЕСКИХ ЗНАНИЙ

Лебедь Ирина Петровна
педагог–исследователь, учитель математики
Учреждение «Академический лицей города Костанай»
г. Костанай, Казахстан
E–mail: irina.lebed.2012@bk.ru

Аңдатпа

Мақаланың өзектілігі цифрлық технологияларды қолдана отырып, білім беру процесіне қойылатын заманауи талаптарға байланысты. Мақсат–математика сабақтарында, үй тапсырмаларын орындау кезінде және сыныптан тыс жұмыстарда цифрлық ортаны құрудың оңтайлы формаларын, құралдары мен әдістерін табу. Мақалада мектептегі білім берудің цифрлық ортасының деңгейлері келтірілген: институционалды, аспаптық, пәндік–дамытушылық; математикалық білім алу шеңберінде пәндік–дамытушылық деңгейдің құрылымдық–мазмұнды мазмұны егжей–тегжейлі сипатталған. Мақаланың авторлық материалының құндылығы математикалық білім деңгейін арттыруға бағытталған сандық құрылғылардың кең ауқымымен анықталады.

Түйінді сөздер: *цифрлық орта, цифрлық орта деңгейлері, математикалық білім, оқушылар, интернет–технологиялар, цифрлық ресурстар, білім беру порталдары.*