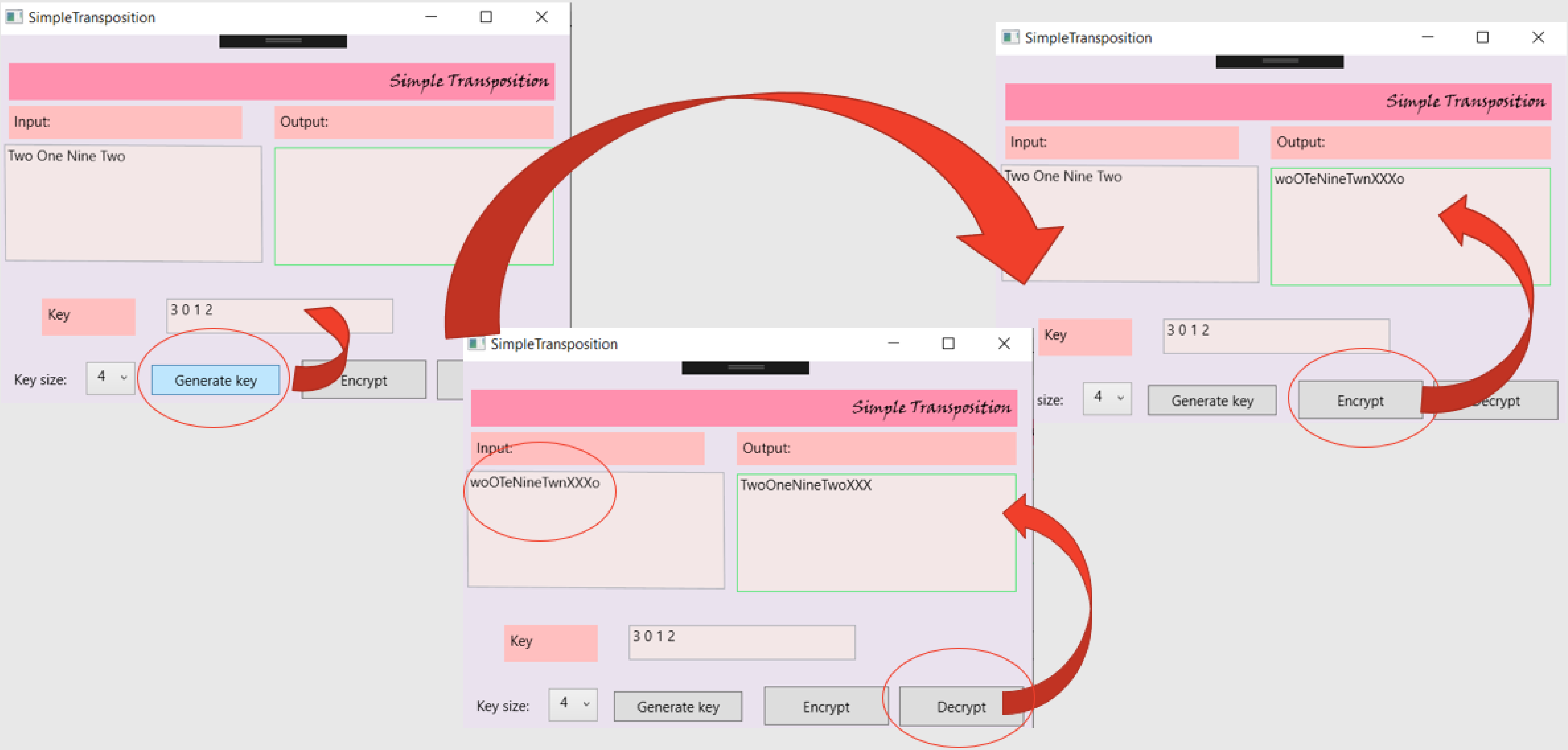
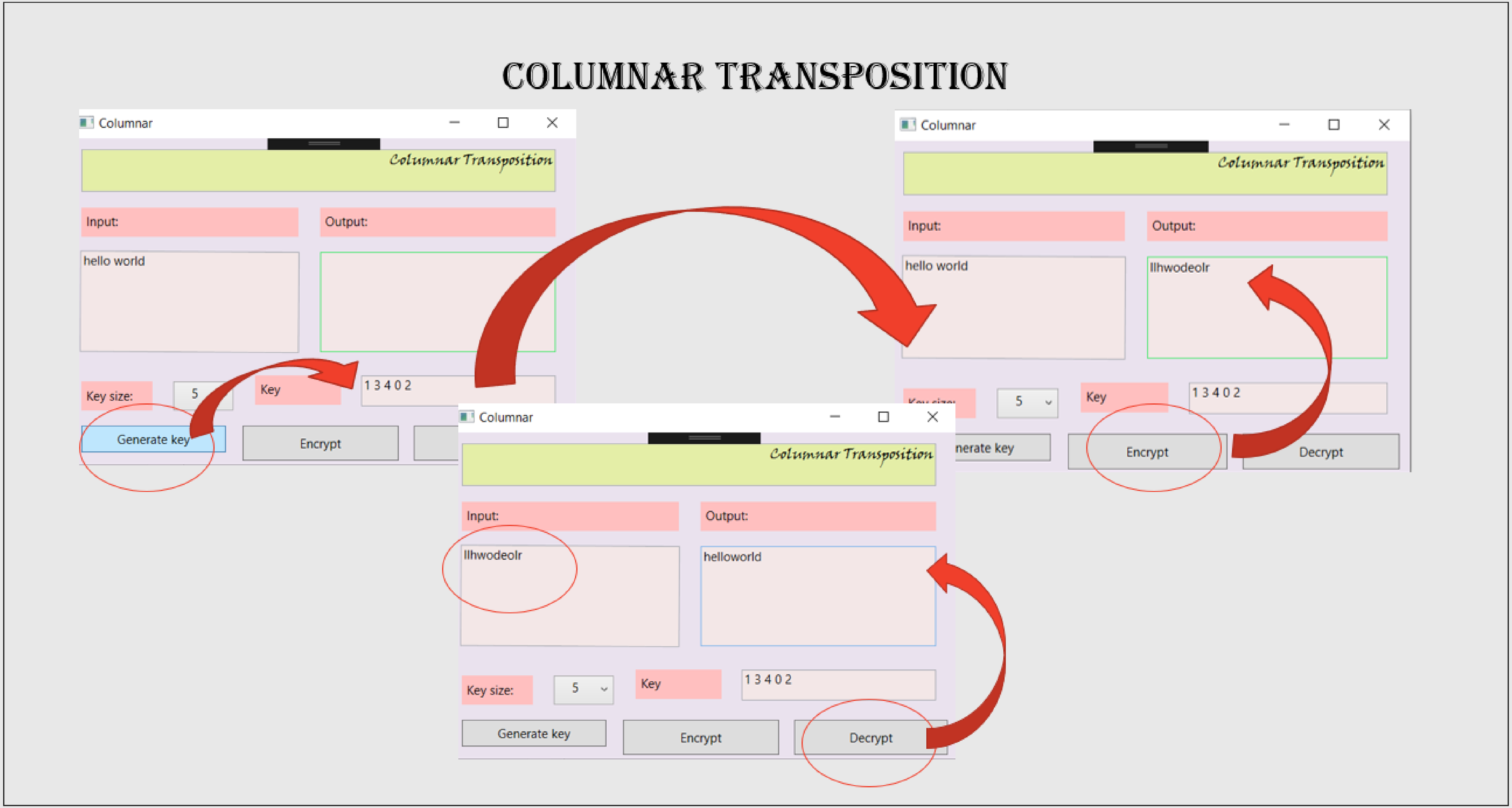
RC4 CIPHER AND ITS CRYPTANALYSIS

Done by: Kakibay A., Akmuratova S.
Checked by: Kudaibergenov A.

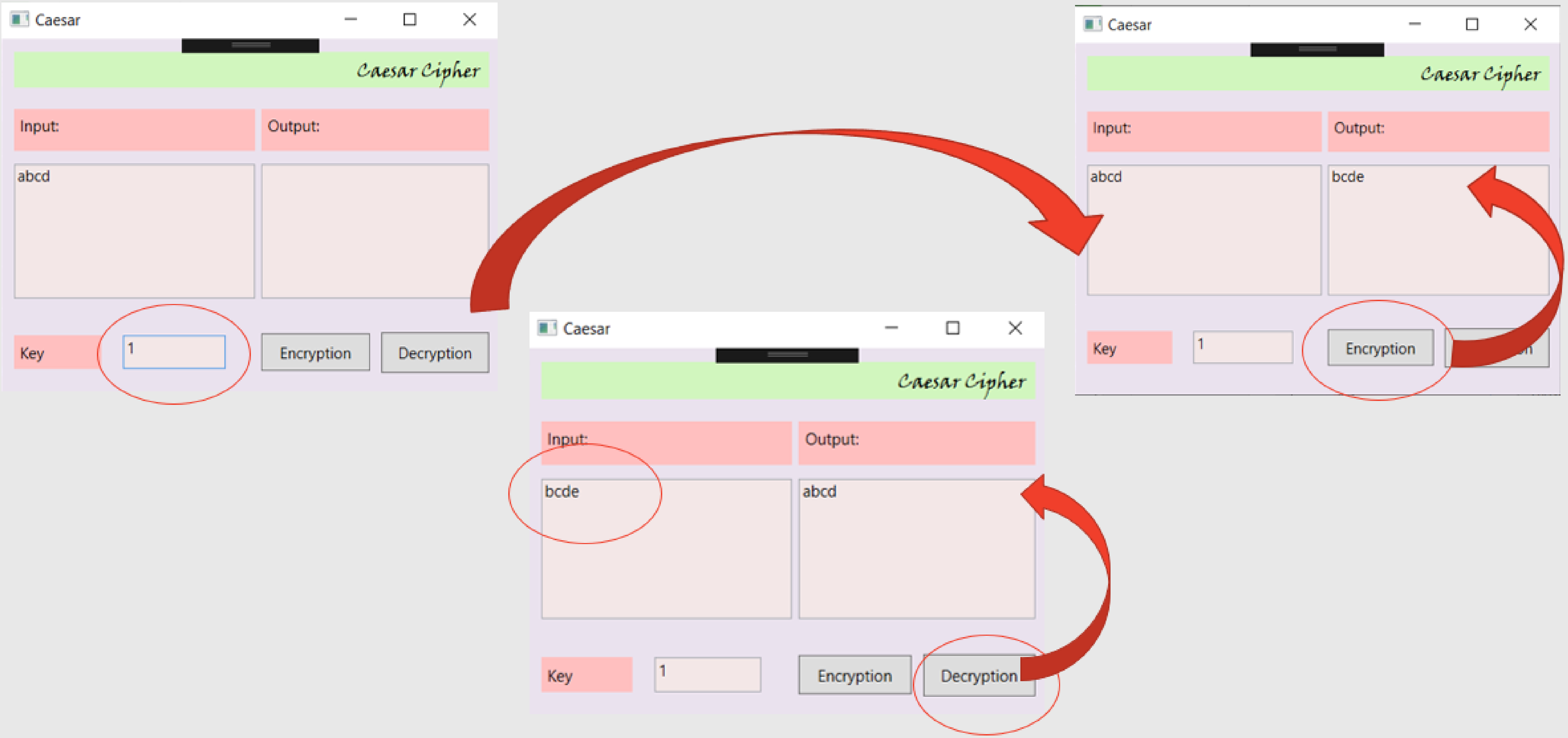
All ciphers and their realizations

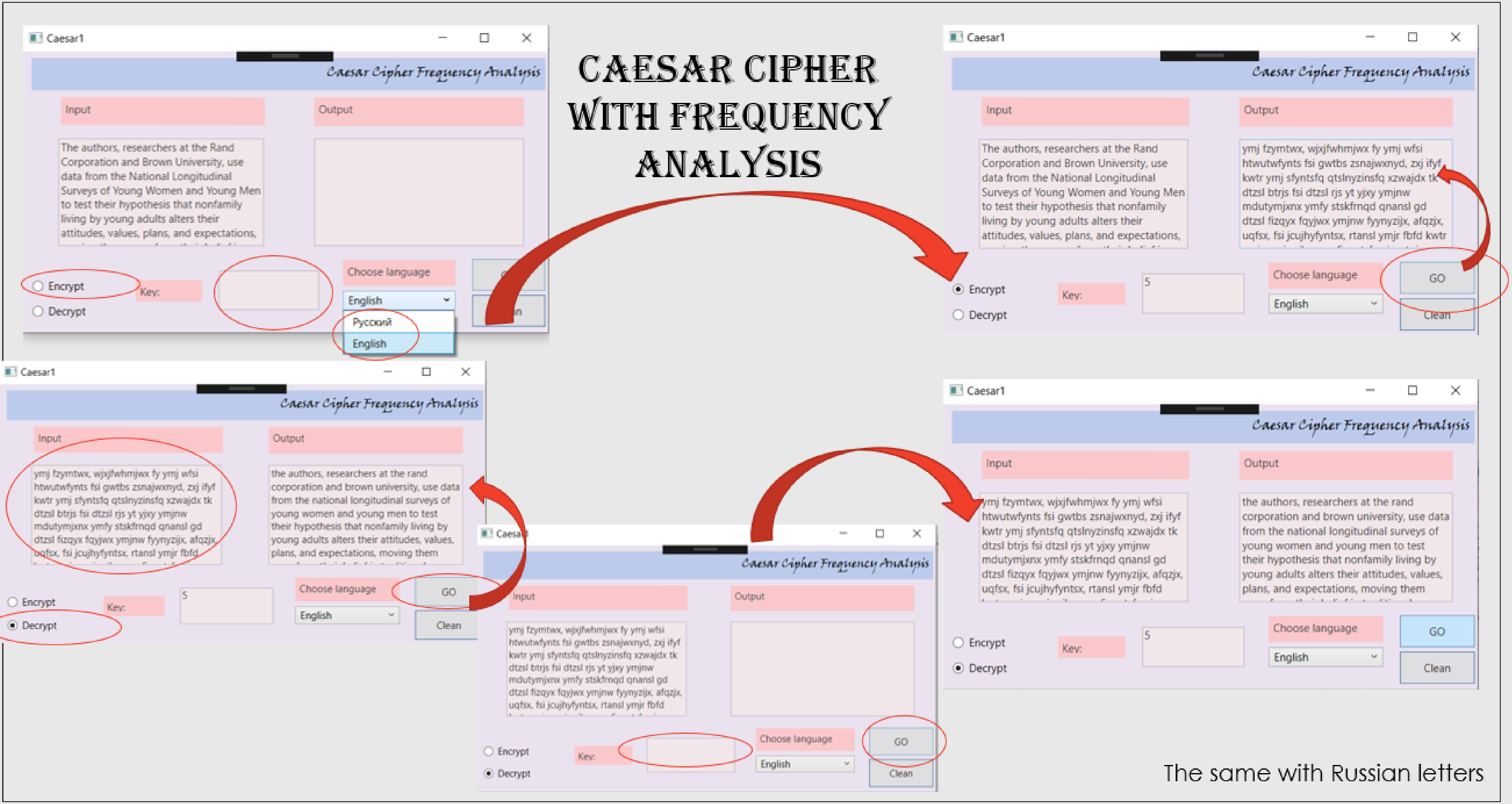
SIMPLE TRANSPOSITION

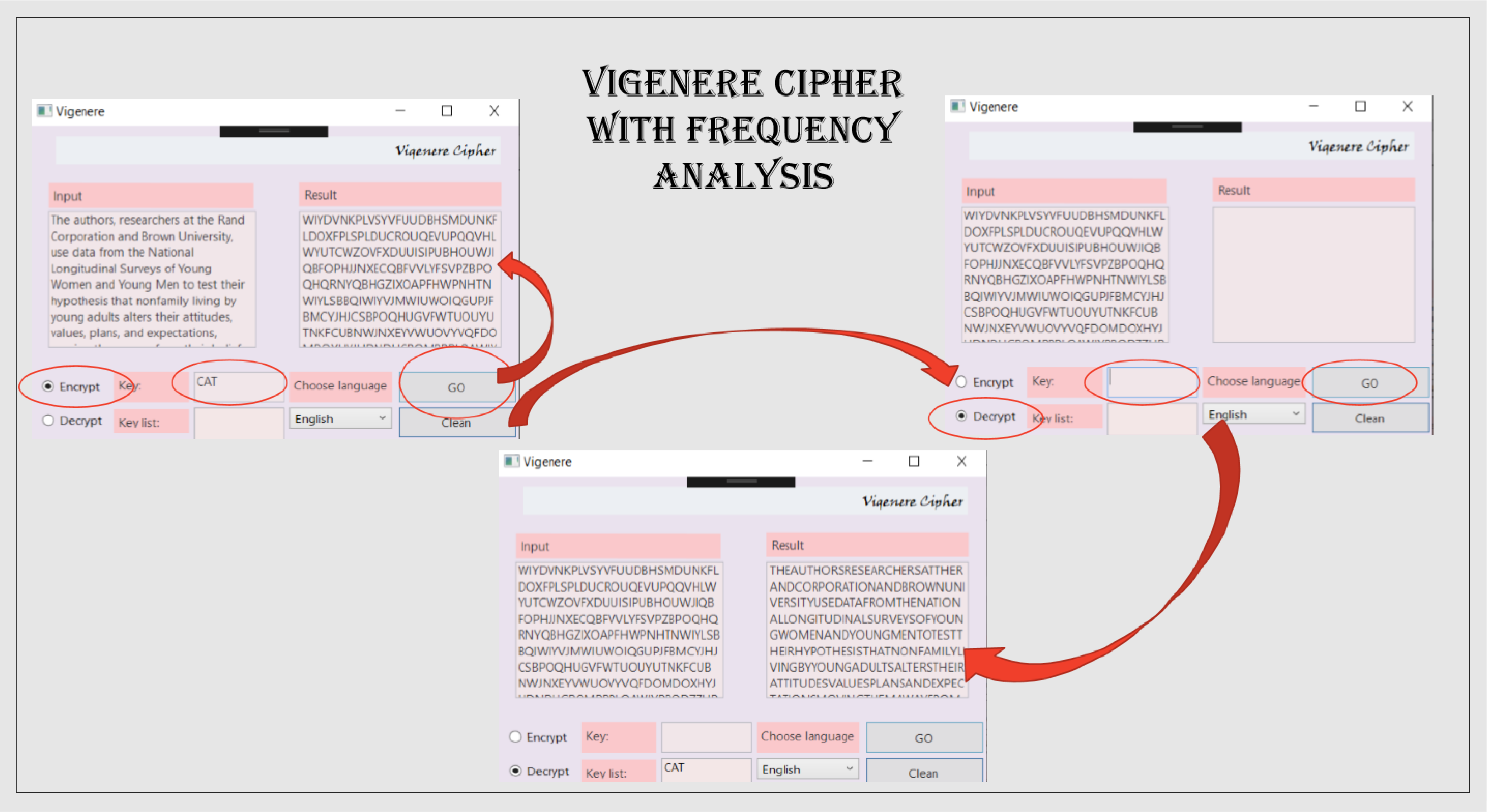


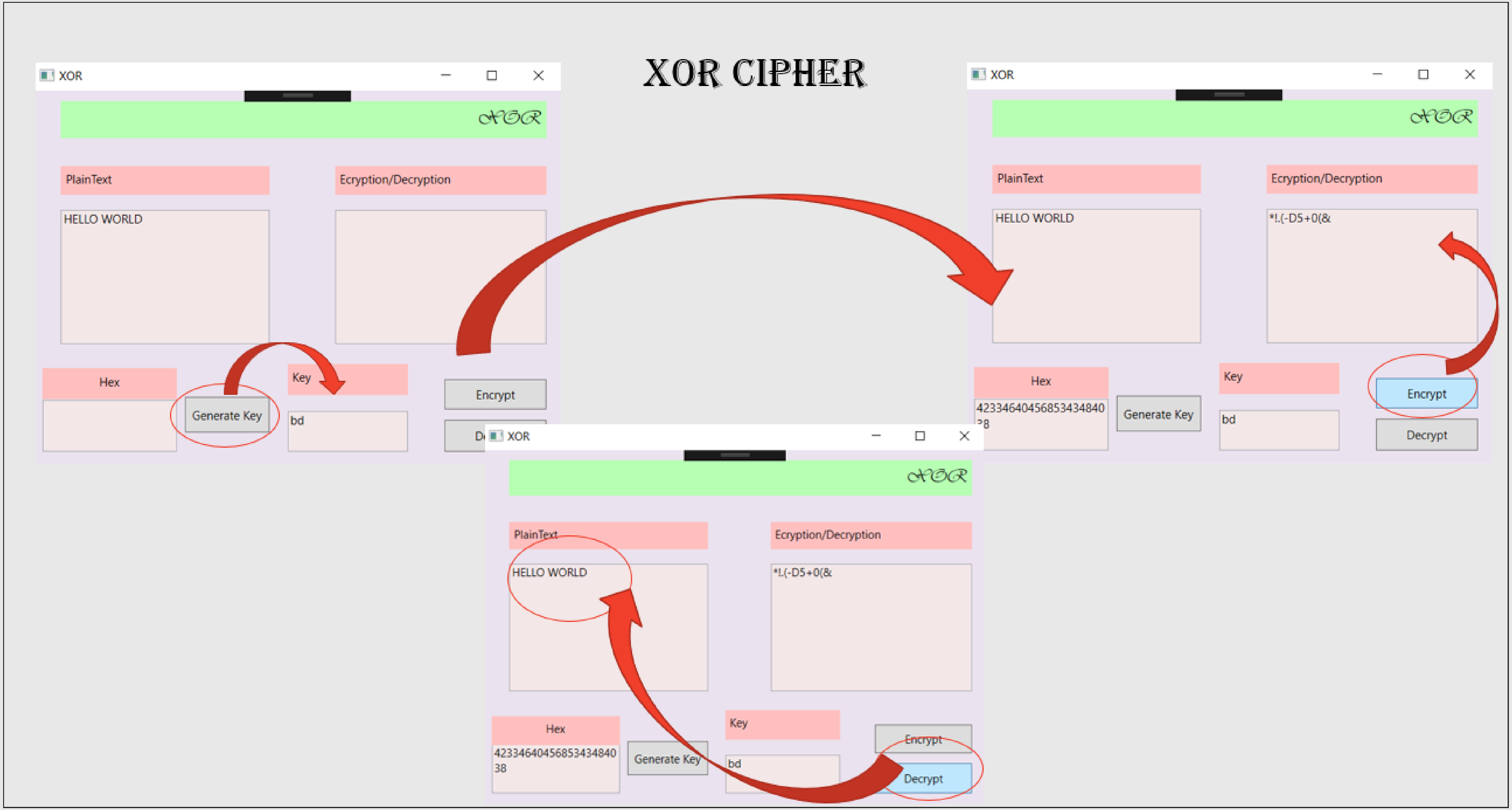

COLUMNAR TRANSPOSITION
Columnar
Columnar Transposition
Input:
Output:
hello world
Key size:
5
Key
1 3 4 0 2
Generate key
Encrypt
Columnar
Columnar Transposition
Input:
Output:
hello world
llhwodeolr
5
Key
1 3 4 0 2
Encrypt
Decrypt
Columnar
Columnar Transposition
Input:
Output:
llhwodeolr
helloworld
Key size:
5
Key
1 3 4 0 2
Generate key
Encrypt
Decrypt

CAESAR CIPHER



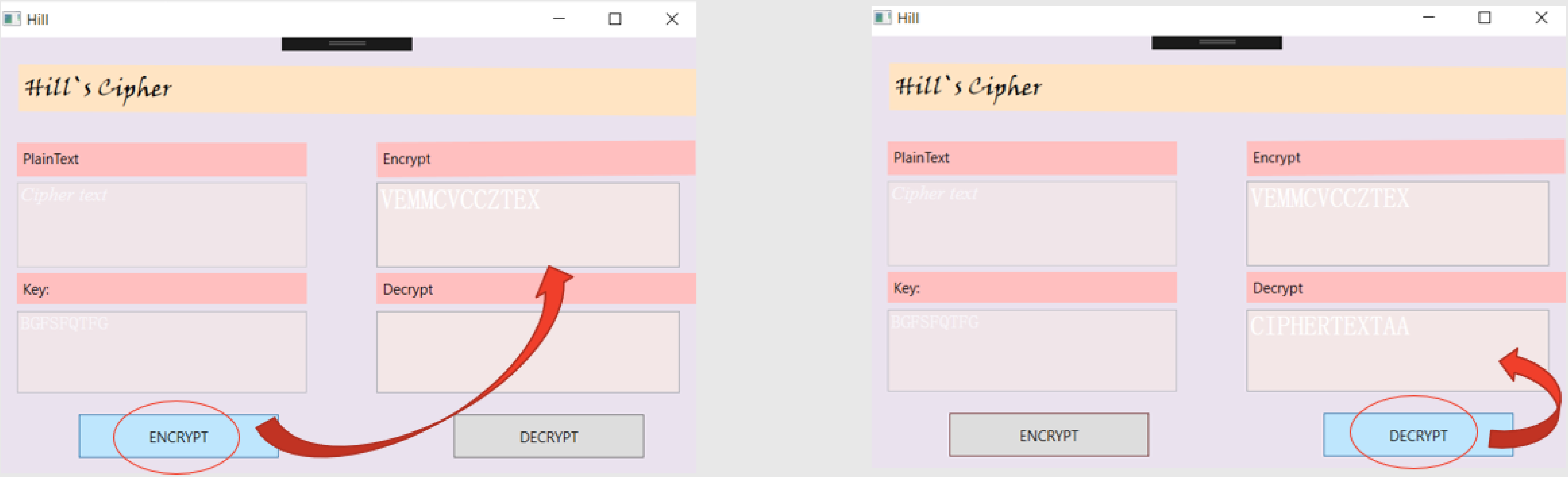

CAESAR CIPHER WITH FREQUENCY ANALYSIS
Caesar1
Caesar Cipher Frequency Analysis
Input
Output
Encrypt
Decrypt
Key:
Choose language
English
Русский
GO
Clean
The same with Russian letters


VIGENERE CIPHER WITH FREQUENCY ANALYSIS
Vigenere
Vigenere Cipher
Input
Result
The authors, researchers at the Rand Corporation and Brown University, use data from the National Longitudinal Surveys of Young Women and Young Men to test their hypothesis that nonfamily living by young adults alters their attitudes, values, plans, and expectations,
WIYDVNKPLVSYVFUUDBHSMDUNKF
LDOXFPLSPLDUCROUQEVUPQQVHL
WYUTCWZOVFXDUUISIPUBHOUWJI
QBFOPHJJNXECQBFVVLYFSVPZBPO
QHQRNYQBHGZIXOAPFHWPNHTN
WIYLSBBQIWIYVJMWIUWOIQGUPJF
BMCYJHJCSBPOQHUGVFWTUOUYU
TNKFCUBNWJNXEYVWUOVYVQFDO
Encrypt
Decrypt
Key:
CAT
Key list:
Choose language
English
GO
Clean
Vigenere
Vigenere Cipher
Input
Result
WIYDVNKPLVSYVFUUDBHSMDUNKFL
DOXFPLSPLDUCROUQEVUPQQVHLW
YUTCWZOVFXDUUISIPUBHOUWJIQB
FOPHJJNXECQBFVVLYFSVPZBPOQHQ
RNYQBHGZIXOAPFHWPNHTNWIYLSB
BQIWIYVJMWIUWOIQGUPJFBMCYJHJ
CSBPOQHUGVFWTUOUYUTNKFCUB
NWJNXEYVWUOVYVQFDOMDOXHYJ
Encrypt
Decrypt
Key:
Key list:
Choose language
English
GO
Clean
Vigenere
Vigenere Cipher
Input
Result
WIYDVNKPLVSYVFUUDBHSMDUNKFL
DOXFPLSPLDUCROUQEVUPQQVHLW
YUTCWZOVFXDUUISIPUBHOUWJIQB
FOPHJJNXECQBFVVLYFSVPZBPOQHQ
RNYQBHGZIXOAPFHWPNHTNWIYLSB
BQIWIYVJMWIUWOIQGUPJFBMCYJHJ
CSBPOQHUGVFWTUOUYUTNKFCUB
NWJNXEYVWUOVYVQFDOMDOXHYJ
THEAUTHORSRESEARCHERSATTHER
ANDCORPORATIONANDBROWNUNI
VERSITYUSEDATAFROMTHENATION
ALLONGITUDINALSURVEYSOFYOUN
GWOMENANDYOUNGMENTOTESTT
HEIRHYPOTHESISTHATNONFAMILYLI
VINGBYYOUNGADULTSALTERSTHEIR
ATTITUDESVALUESPLANSANDEXPEC
Encrypt
Decrypt
Key:
Key list:
CAT
Choose language
English
GO
Clean

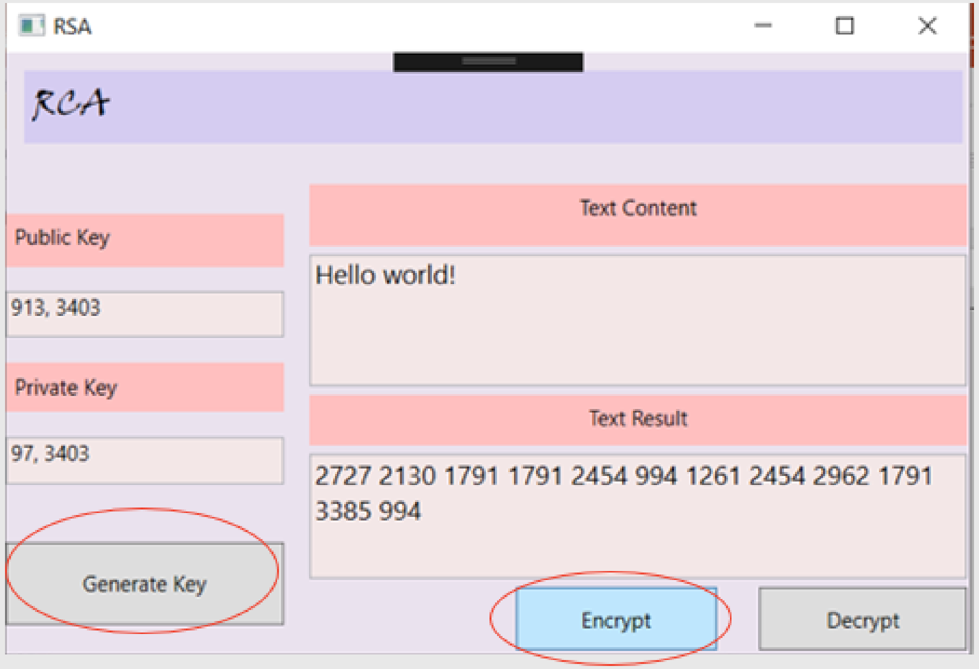


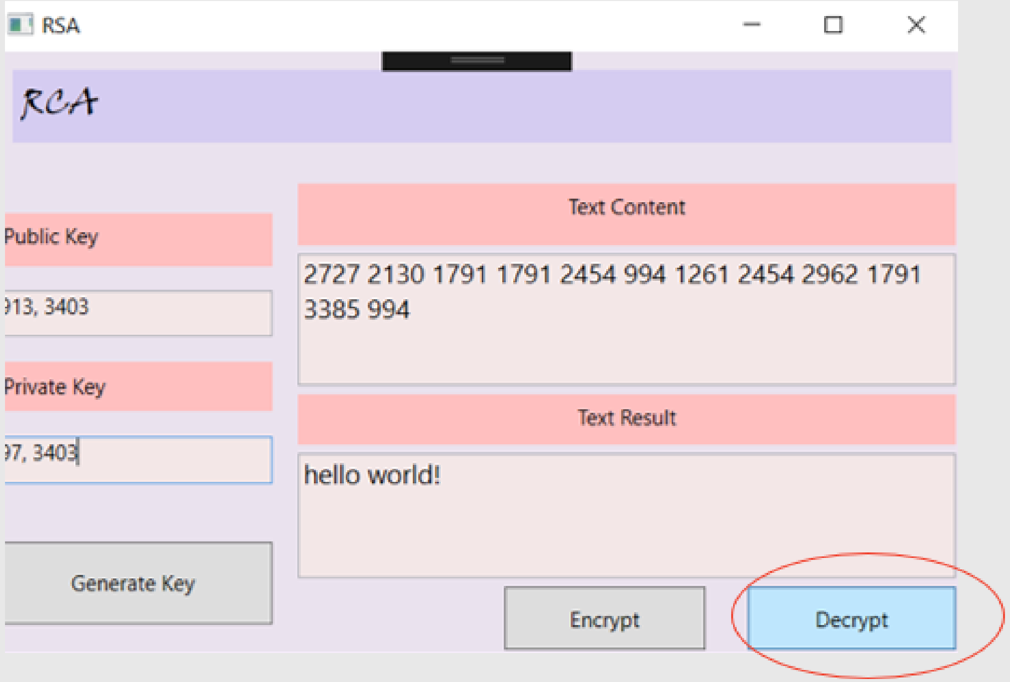
XOR CIPHER
XOR
XOR
PlainText
Ecryption/Decryption
HELLO WORLD
Hex
Generate Key
Key
bd
Encrypt
XOR
XOR
PlainText
Ecryption/Decryption
HELLO WORLD
*!.(-D5+0(&
Hex
42334640456853434840
38
Generate Key
Key
bd
Encrypt
Decrypt
XOR
XOR
PlainText
Ecryption/Decryption
HELLO WORLD
*!.(-D5+0(&
Hex
42334640456853434840
38
Generate Key
Key
bd
Encrypt
Decrypt

HILL'S CIPHER

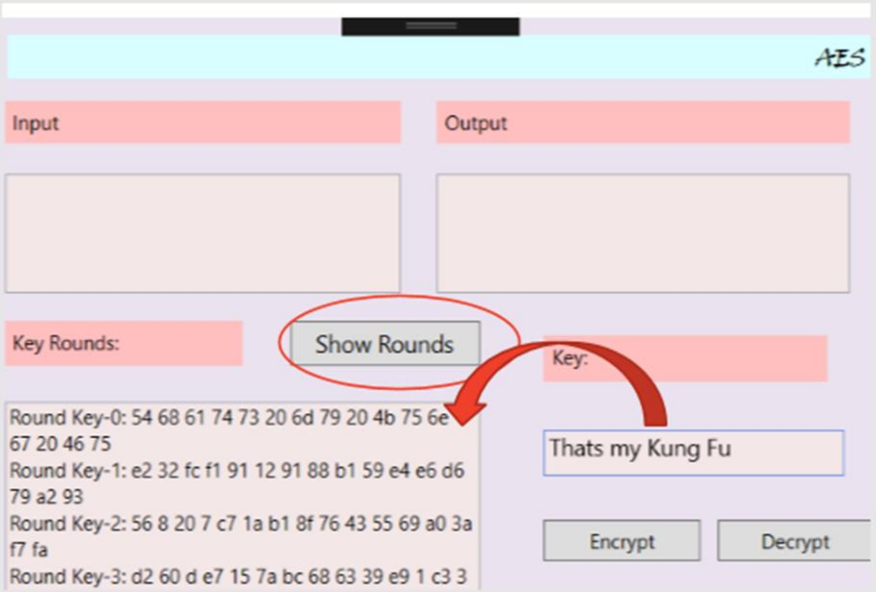


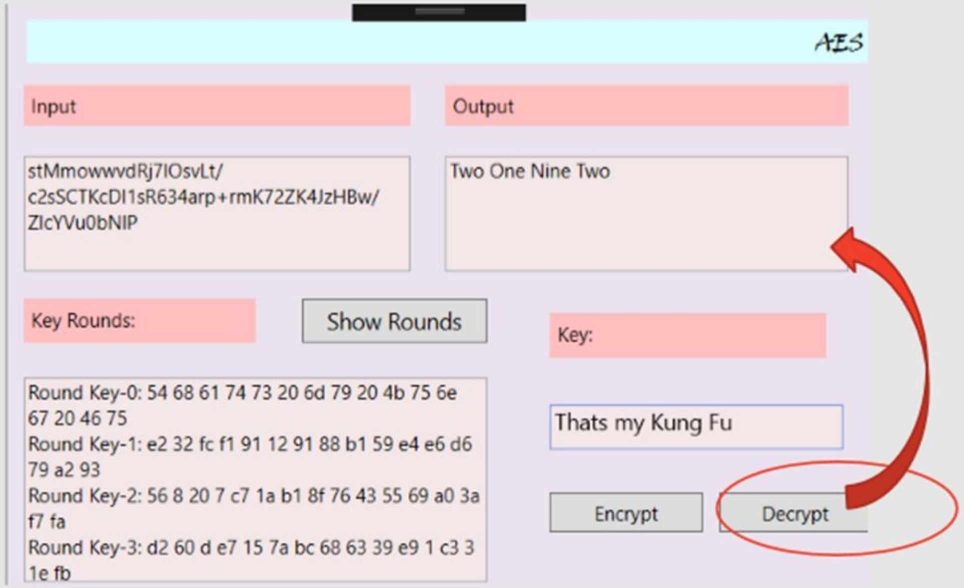
RSA CIPHER


RSA
RCA
Public Key
913, 3403
Private Key
97, 3403
Generate Key
Text Content
Hello world!
Text Result
2727 2130 1791 1791 2454 994 1261 2454 2962 1791 3385 994
Encrypt
Decrypt


RSA
RCA
Public Key
913, 3403
Private Key
97, 3403
Generate Key
Text Content
2727 2130 1791 1791 2454 994 1261 2454 2962 1791 3385 994
Text Result
hello world!
Encrypt
Decrypt

AES CIPHER





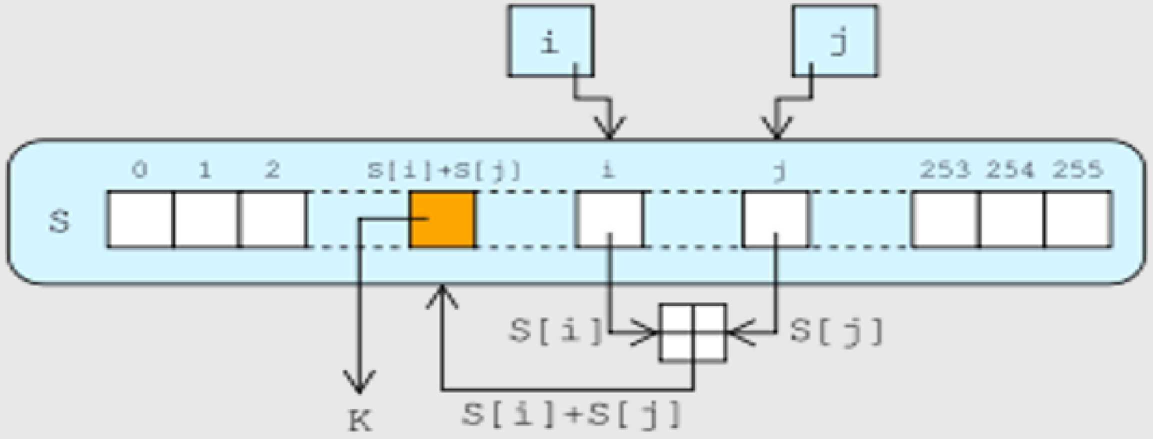
28.05.2020

RC4 CIPHER

RC4 is a stream cipher widely used in various information security systems. The RC4 algorithm is based on a pseudo-random bit generator. The key is written to the input of the generator, and pseudo-random bits are read at the output. The key length can range from 40 to 2048 bits. The generated bits have a uniform distribution.

The main advantages of the cipher:

- high speed operation;
- variable key size.



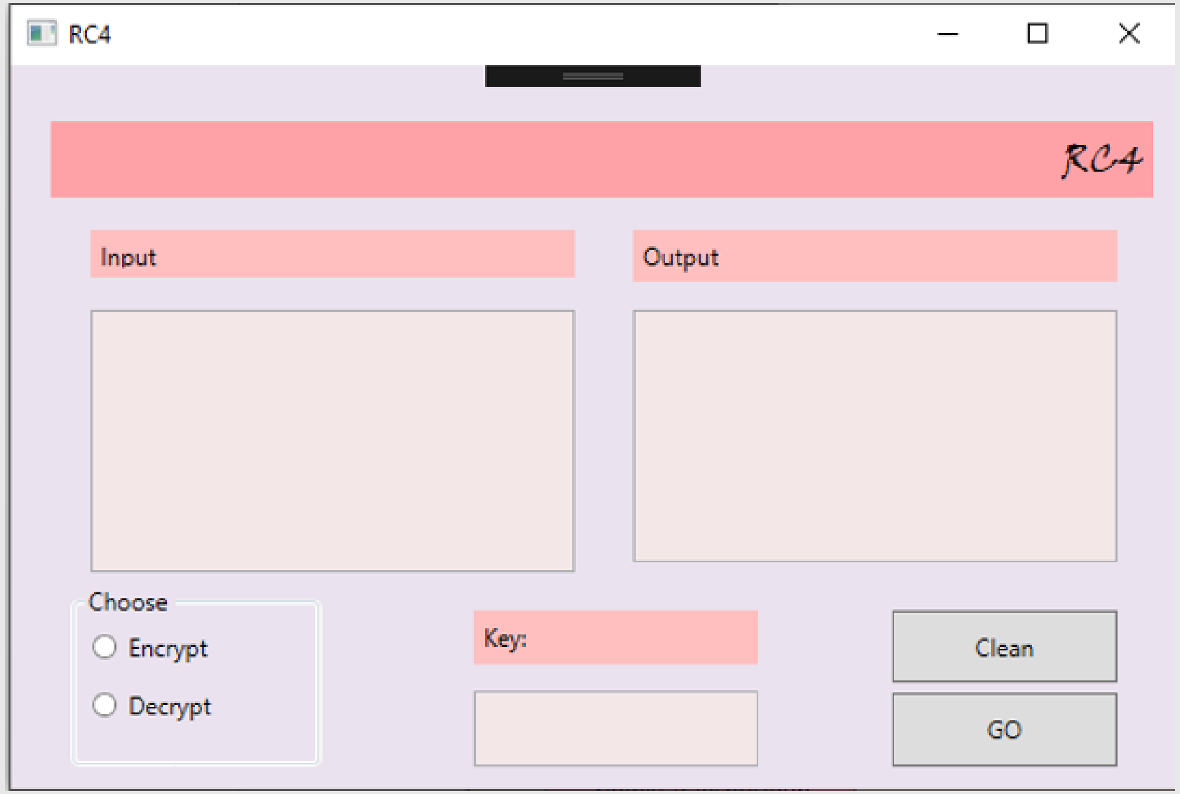
Algorithm of RC4

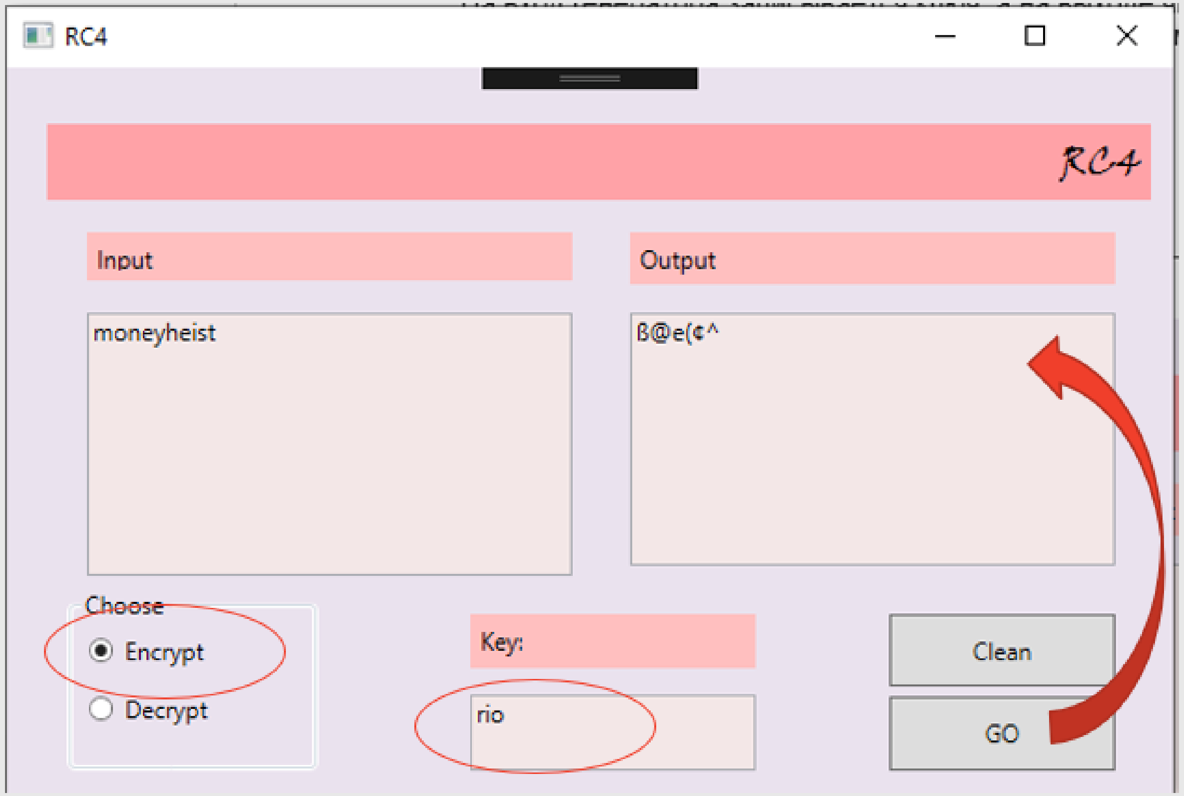
1. Function is generating sequence of bits k_i
2. To encrypt $c_i = m_i \oplus k_i$, for decryption $m_i = (m_i \oplus k_i) \oplus k_i$
3. "Key-scheduling algorithm". In this algorithm we dive own key and key length. First, we fill the array box then this array is shuffled by permutations defined by the key. We need to be sure that box has the same value as was given during the initialization. Next, j = (key[i % key.Length] + box[i] + j) % 256 will be performed, then just swap box[i] and box[j].
4. Next step is pseudo-random generation algorithm. Here in one loop is defining one n-bits text from the keystream, then just swap box[y] and box[j]. After key will do XOR with plaintext.

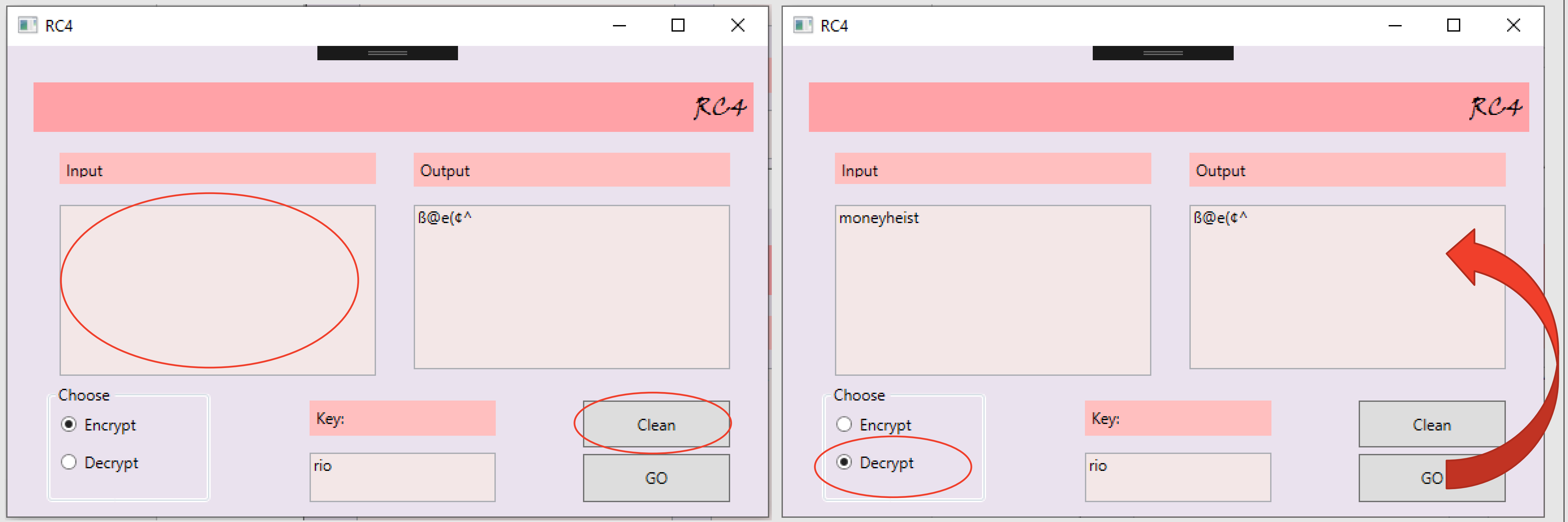
REALIZATION OF ALGORITHM

```
public string EncrDecr(string input, string key)
        {
            StringBuilder result = new StringBuilder();
            int x, y, j = 0;
            int[] box = new int[256];
            for (int i = 0; i < 256; i++)//initialization of S-box
                box[i] = i;
            for (int i = 0; i < 256; i++)
            {
                j = (key[i % key.Length] + box[i] + j) % 256;
                x = box[i];
                box[i] = box[j];
                box[j] = x;
            }
            for (int i = 0; i < input.Length; i++)//pseudo-random generation algorithm
            {
                y = i % 256;
                j = (box[y] + j) % 256;
                x = box[y];
                box[y] = box[j];
                box[j] = x;
                result.Append((char)(input[i] ^ box[(box[y] + box[j]) % 256]));
            }
            return result.ToString();
        }
```

RESULTS:


RC4
RC4
Input
Output
Choose
Encrypt
Decrypt
Key:
Clean
GO

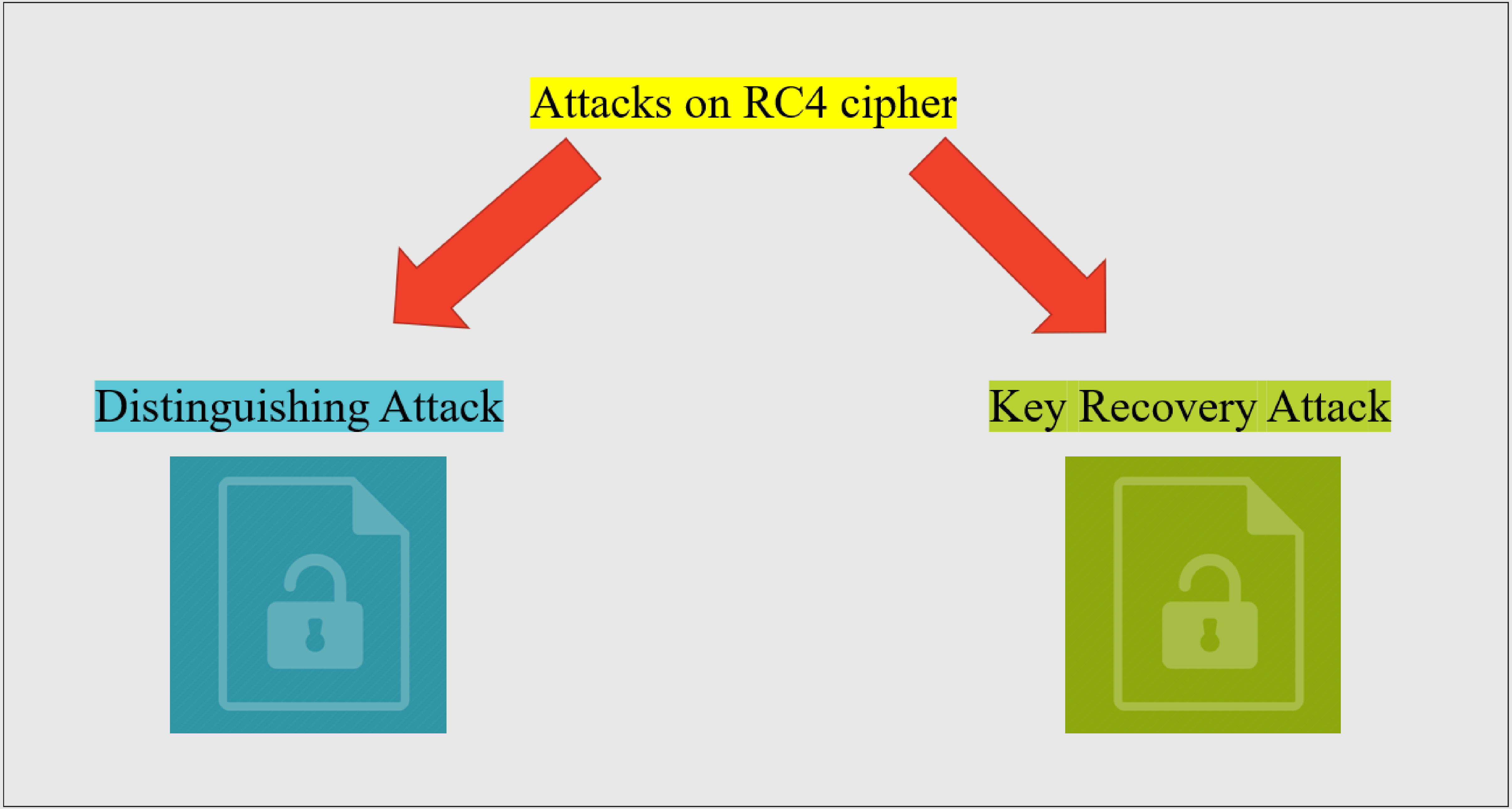

RC4
RC4
Input
Output
moneyheist
ß@e(¢^
Choose
Encrypt
Decrypt
Key:
rio
Clean
GO


RC4
RC4
Input
Output
ß@e(¢^
Choose
Encrypt
Decrypt
Key:
rio
Clean
GO
RC4
RC4
Input
Output
moneyheist
ß@e(¢^
Choose
Encrypt
Decrypt
Key:
rio
Clean
GO

CRYPTANALYSIS OF RC4

Cryptanalysis is an attempt to decipher cipher text without key.

RC4 Cryptanalysis:
- XOR is a weak operation;
- Security depends entirely on the randomness of the state vector;
- States are pseudo-random
  - They will repeat with time


Attacks on RC4 cipher
Distinguishing Attack
Key Recovery Attack

The attacks are based on weakness:

- Non-randomness property of initial variable;
- Low diffusion property of key-scheduling algorithm and pseudo-random generation algorithm

Distinguishing attack ►

Input: First 2 words of output corresponding 2^{4*n} randomly selected secret key.

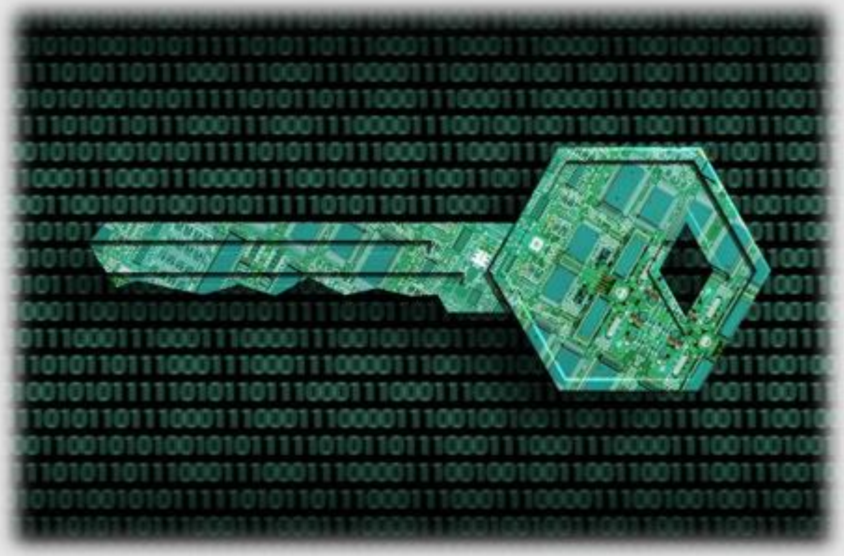
Output: To distinguish between cipher outputs and random source:

1. Generate $Output^k[0]$ and $Output^k[1]$

2. $S = \frac{\sum k([Output[0] \oplus Output[1]])}{2^{(2*n)}}$

3. $S \geq 1/2$, the algorithm that was analyzed will be our RC4

Key Recovery attack▶



Input: Two initial vectors IV1 and IV2

Output: To distinguish between cipher outputs and random source:

1. Guess SK[0] = $\widetilde{SK_0}$
2. Calculate $[IV_1[0]]0 \ldots 7 = \widetilde{-SK_0} \bmod 2^8$
3. Choice differential vectors $\Delta_{IV}[0] = \Delta$
4. Output keystream 2^8 words need to be generated, Output1[j] and Output2[j]

$$\begin{cases} IV_1[0] = IV_2[0] \oplus \Delta_{IV}[0] \\ IV_1[i] = IV_2[i] \end{cases}$$

5. The output differential vector is calculating like ΔOutput[j] = Output1[j] ⊕ Output2[j]
6. In case when ΔOutput[j] = 0x00 00 00 00, $\widetilde{SK_0}$ will be the least important byte of secret key with probability close to 1, else go to 1st step.

Summary:

- Knowing the entire state at a given time allows knowledge of all future values;
- Knowing the entire initial state effectively breaks the cipher;
- Initial state depends only upon the key;
- The key uniquely determines the keystream.

THANK YOU,

FOR YOUR ATTENTION :D