Rakieta_1_BSK_2017

1. Szyfrogram o prezydenta Kennedy został złożony z prostego podstawienia:
C = RGJJG MVKTO TZPGT STBGP CATJW PGOCM GJS
Co to jest odpowiednie zwykłego tekstu?

Na czuja, ale podobno trzeba policzyć która litera najczęściej występuje (G → 6) i próbować podstawić coś z {A,E,I,O}

RGJJGMV KTO T ZPGTS TBGPCATJ WPGOCMGJS
M = KENNEDY WAS A GREAT AMERICAN PRESIDENT

https://books.google.pl/books?id=j0LxBwAAQBAJ&pg=PA25&lpg=PA25&dq=RGJJG+MVKTO+TZPGT+STBGP+CATJW+PGOCM+GJS&source=bl&ots=N48F8UrJM_&sig=WVRd4Pc97mBMNRZMTF-C7HKRGSM&hl=pl&sa=X&ved=0ahUKEwjxjo7j0qLTAhUSIlAKHQt9AKAQ6AEIIzAA#v=onepage&q=RGJJG%20MVKTO%20TZPGT%2

2. Poniższy tekst tajny C został otrzymany za pomocą algorytmu „rail-fence”
C=IFRAINNOMTO
Jak wygląda odpowiadający mu tekst jawny M?

I		F		R		A		I		N
	N		O		M		T		O	

M = INFORMATION

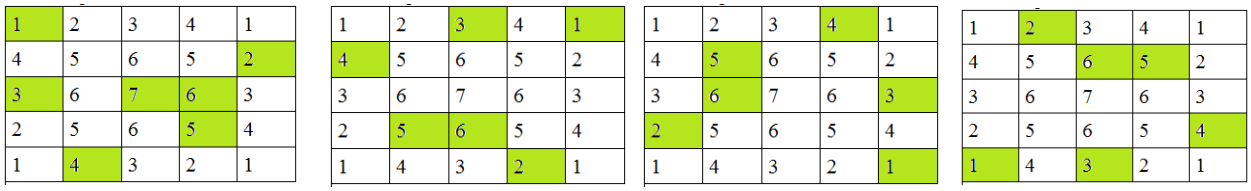
3. Niech dany będzie następujący tekst jawny M=IT IS A SECRET MESSAGE oraz szyfr przestawieniowy o następujących regułach:
Reguła „Write-in” (zapisu): Tekst jawny jest zapisywany w kolejnych wierszach macierzy (macierz o wymiarach: 3 wiersze oraz 6 kolumny)
Reguła „Take-off” (odczytu): Odczytywanie kolumn w kolejności 2-1-3-6-4-5.
Jaki jest odpowiadający dla M szyfrogram C?

1	2	3	4	5	6
I	T	I	S	A	S
E	C	R	E	T	M
E	S	S	A	G	E

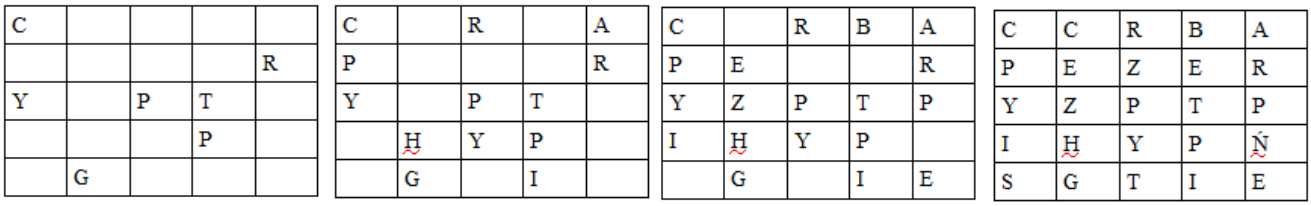
C = TIISASCERMETSESEAG

4. Zwykły tekst M = CRYPTPGRAPHY I BEZPIECZEŃSTWO DANYCH powinny być szyfrowane z szyfrem transpozycji „turning grille”, z kluczem Co to jest odpowiedni szyfrogram C?

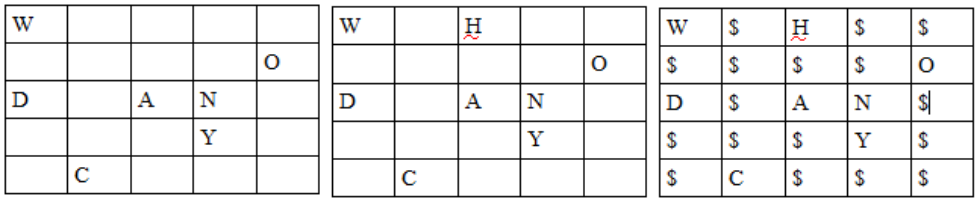
1				
				2
3		**7**	**6**	
			5	
	4			



W utworzone miejsca wstawiamy kolejno litery z hasła



Jeśli zapełnimy miejsce tworzymy nową macierz i robimy wszystko od początku.



Jak coś zostanie to wrzucamy $, ażeby deszyfrowanie przyjemniejszym było :)

C = CCRBAPEZERYZPTPIHYPŃSGTIEW$H$$$$$OD$AN$$$$Y$$C$$$

5. Niech F odwzorowuje standardowy alfabet angielski M={*A,B,...,Z*} w alfabet szyfrogramu C={*A,B,...,Z*} zgodnie z zależnością:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
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	C	D	E	F	G	H	J	N	P	Y	A	R	M	O	L	I	K	Q	S	T	U	V	W	X	Z

Niech C = QFQQNXB jest szyfrogramem otrzymanym z odpowiadającego mu tekstu jawnego M. Jaki jest tekst jawny M?

Zaznaczamy Q,F,N,X,B i podstawiamy litery wyżej

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
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	C	D	E	F	G	H	J	N	P	Y	A	R	M	O	L	I	K	Q	S	T	U	V	W	X	Z

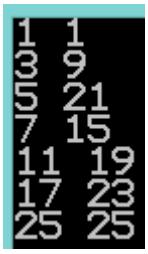
M = SESSIYA

6. Jaki jest tekst jawny M dla szyfrogramu C=XYZIJSY, otrzymanego za pomocą szyfru podstawienowego *c*=(*a*+*k*) *mod n* dla klucza *k*=5 oraz standardowego alfabetu angielskiego?
Jaka jest wartość *k'* dla procesu deszyfracji na podstawie poniższego wzoru?

a=(*c*+*k'*) *mod n.*
k'=*(n-k)* => *k' = 21*
X = 23, więc (23 + 21) mod 26 = 18 = > S
Wersja dla leniwych? W alfabecie 5 liter do tyłu.

7. Jaki jest tekst jawny M dla szyfrogramu C=CFIJMNF, otrzymanego za pomocą szyfru podstawienowego *c*=(k x a) *mod n* dla klucza *k*=3 oraz standardowego alfabetu angielskiego?
Jaka jest wartość *k'* dla procesu deszyfracji na podstawie poniższego wzoru?
***a*=(*c* x *k'*) mod n.**

Wygenerowana para kluczy (jeśli k = 3 to k' = 9 i odwrotnie)



Jakby ktoś nie zapamiętał i na kolosie chciał odpalić ideone:

```
static void Main(string[] args)
{
    for (int i=1;i<=26;i++)
    {
        int x = SearchK2(i);
        if (x>=i && x!=0)
            Console.WriteLine(i + " " + SearchK2(i));
    }
    Console.ReadKey();
}

public static int SearchK2(int k)
{
    for (int i = 1; i <= 26; i++)
        if ((i * k) % 26 == 1)
            return i;
    return 0;
}
```

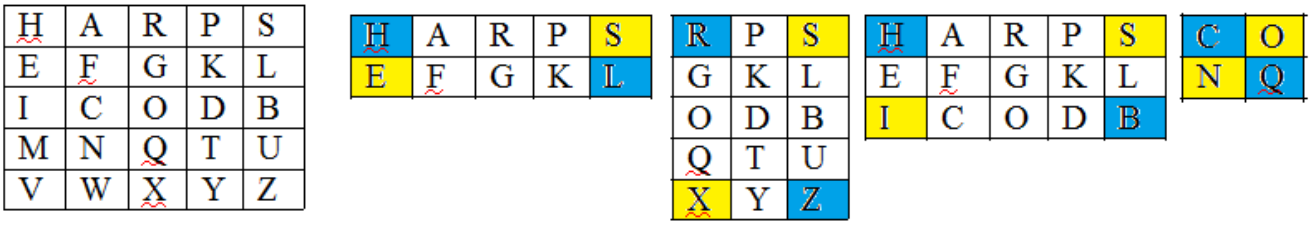
8. Jaka jest wartość k_1' i k_0' dla procesu deszyfracji $a=(k_1'c+k_0')$ *mod n* na podstawie poniższego wzoru szyfracji $c=(7xa+3)$ *mod n*?

$k_0' = 26-3 = 23$
$k_1' = 15$

9. Zakoduj następujący tekst jawny M=SESSION, w oparciu o algorytm Playfair dla klucza przedstawionego poniżej.

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

1. Dzielimy słowo do zaszyfrowania na pary → SE-SS-IO-N
2. Jeśli sąsiednie litery się powtarzają wstawiamy pomiędzy nie X → SE-SX-SI-ON
3. Jeśli mamy nieparzystą liczbę i na końcu litera nie ma pary dodajemy X (nie dotyczy)
4. Dzielimy otrzymane pary na sektory SE-SX-SI-ON



Otrzymane hasło → C = XL-RZ-HB-CQ

10.Zakoduj następujący tekst jawny *M*= IT IS A SECRET MESSAGE, w oparciu o algorytm Bifid Cipher dla klucza przedstawionego poniżej.

	1	2	3	4	5
1	H	A	R	P	S
2	E	F	G	K	L
3	I	C	O	D	B
4	M	N	Q	T	U
5	V	W	X	Y	Z

Dzielimy tekst na 5
ITISA SECRE TMESS AGE
Wpisujemy

	I	T	I	S	A		S	E	C	R	E		T	M	E	S	S		A	G	E
W	3	4	3	1	1		1	2	3	1	2		4	4	2	1	1		1	2	2
K	1	4	1	5	2		5	1	2	3	1		4	1	1	5	5		2	3	1

Spisujemy wiersz → kolumna, wiersz → kolumna itd.
3431114152 1231251231 4421141155 122231
Dzielimy otrzymany ciąg co dwa
34-31-11-41-52-12-31-25-12-31-44-21-14-11-55-12-22-31
Otrzymujemy nowe koordynaty liter

C=DIHMWAILAHLAITEPHZAFI

11. Zakoduj następujący tekst jawny *M*=MESSAGE, w oparciu o algorytm The Stradding Checkerboard dla klucza

	9	8	2	7	0	1	6	4	3	5
	A	T		O	N	E		S	I	R
2	B	C	D	F	G	H	J	K	L	M
6	P	Q	U	V	W	X	Y	Z	.	/

25-1-4-4-9-20-1

C = 251449201

12. Zakoduj następujący tekst jawny M=VIGENERE, w oparciu o algorytm Vigenere dla klucza:
12.1. *Straight* klucz *k*=SIX;
12.2. *Progressive* klucz *k*=SEVEN;
12.3. *Auto* klucz *k*=FIVE.

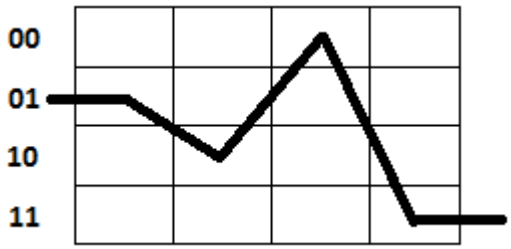
VIGENERE

SIXSIXSI
SEVENTFW(bo S+1 = T, E+1 = F, V+1 = W)
FIVEVIGE

I juz normalny Vigenere V+S mod 26 itd.

13. Zawartość dla *rotor mashine* są przy użyciu dla procesu szyfracji.
Co to jest odpowiednie zawartość dla *rotor mashine* przy użyciu dla procesu deszyfracji?

01
10
00
11



Coś podobnego było o Enigmie u Mazurka.
Wchodzi przez 00 i wychodzi 11

Aby odszyfrować droga musi być powrotna więć → 11,00,10,01

14. Jaka jest wartość entropii dla trzech zdarzenia *A*, *B*, *C* z odpowiednimi prawdopodobieństwami *P*(*A*) = 1/4 and *P*(*B*) = *P*(*C*) = 3/8.

To jest minus z sumy P(x) * log2 (P(x))

Równanie : $-\left(\frac{1}{4}\log_2\left(\frac{1}{4}\right)+\frac{3}{8}\log_2\left(\frac{3}{8}\right)+\frac{3}{8}\log_2\left(\frac{3}{8}\right)\right)$

Po prostych przekształceniach : $-\frac{\log_2\left(\frac{27}{2048}\right)}{4}$

Dla tych z wolphramem lub kalkulatorem na kolosie :
1.561278124459132863909695792039137618430139194230639204658