ZAD.1.(12 pkt.)

Każdą literę tekstu przekształcono w liczby = t korzystając z tabeli znaków ASCII. Na tak otrzymanych liczbach wykonano operację szyfrowania i otrzymano zaszyfrowane postaci tych liczb = c.

Do szyfrowania użyto klucza publicznego (e, n) = (7, 143).

Po zaszyfrowaniu otrzymano ciąg liczb c: 124, 69, 65, 72,123, 54, 65, 89, 35, 108, 110.

Rozszyfrowywanie podanych liczb c wykonujemy kluczem prywatnym RSA***:*** **(d, n) = (103,143), stosując wzór: $t = c^d \bmod n$.**

Korzystając z podanego poniżej przykładu rozszyfruj podane liczby a następnie odczytaj i podaj zakodowany tekst. Przedstaw wszystkie obliczenia.

Przykład:

Otrzymaliśmy zakodowaną wiadomość o wartości c = 7. Jesteśmy w posiadaniu klucza prywatnego (d, n) = (103,143), który służy do rozszyfrowywania wiadomości zakodowanych kluczem publicznym (e, n) = (7, 143).

Wykonujemy następujące operacje:

$t = 7^{103}$ **mod** 143 [reszta z dzielenia liczby 7^{103} przez 143]

Potęga jest zbyt duża, aby można ją było w normalny sposób obliczyć. Jednakże nas nie interesuje wartość liczbowa potęgi, a jedynie reszta z dzielenia jej przez 143. Możemy więc rozłożyć potęgę na iloczyn składników o wykładnikach równych kolejnym potęgom liczby dwa:

7^{103} **mod** 143 = $7^{64 + 32 + 4 + 2 + 1}$ **mod** 143 =

(7^{64} **mod** 143) × (7^{32} **mod** 143) × (7^4 **mod** 143) × (7^2 **mod** 143) × 7 **mod** 143

7^1 **mod** 143 = 7

7^2 **mod** 143 = (7^1 **mod** 143)^2 **mod** 143 = 49 **mod** 143 = 49

7^4 **mod** 143 = (7^2 **mod** 143)^2 **mod** 143 = 49^2 **mod** 143 = 113

7^8 **mod** 143 = (7^4 **mod** 143)^2 **mod** 143 = 113^2 **mod** 143 = 42

7^{16} **mod** 143 = (7^8 **mod** 143)^2 **mod** 143 = 42^2 **mod** 143 = 48

7^{32} **mod** 143 = (7^{16} **mod** 143)^2 **mod** 143 = 48^2 **mod** 143 = 16

7^{64} **mod** 143 = (7^{32} **mod** 143)^2 **mod** 143 = 16^2 **mod** 143 = 113

Do wyliczenia potęgi bierzemy tylko te reszty, które występują w sumie potęg liczby dwa:

$t = 7^{103}$ **mod** 143 = (113 × 16 × 113 × 49 × 7) **mod** 143 = 123.

ZAD.2. (12 pkt)

26- literowy alfabet łaciński podzielono na pięć grup liter odpowiednio po pięć liter w czterech pierwszych grupach oraz sześć liter w ostatniej- piątej grupie. Z tak utworzonych grup liter utworzono szyfr 5-ułamkowy. Szyfrem tym zaszyfrowano pewien tekst w języku angielskim, cytat oraz imię i nazwisko jego autora. Po zaszyfrowaniu tekst ma postać:

$$\left(\frac{3}{1}\cdot\frac{5}{3}+\frac{4}{1}:\frac{5}{1}\cdot\frac{4}{4}\right)+\left(\frac{1}{1}+\frac{3}{4}-\frac{5}{1}\right)-\frac{1}{1}+\left[\left(\frac{1}{4}:\frac{1}{5}-\frac{6}{5}:\frac{6}{5}\right)-\frac{2}{3}+\frac{5}{1}\right]+\frac{1}{1}+\left[\left(\frac{2}{2}:\frac{1}{1}-\frac{3}{3}\cdot\frac{5}{1}\right):\left(\frac{5}{2}\cdot\frac{1}{5}+\frac{4}{4}-\frac{5}{4}\right)\right]:\left(\frac{2}{3}-\frac{4}{2}+\frac{1}{3}\cdot\frac{5}{1}\right)-\left(\frac{1}{1}+\frac{4}{3}\cdot\frac{5}{5}\right)+\left(\frac{5}{3}-\frac{5}{4}+\frac{3}{2}\cdot\frac{5}{1}+\frac{3}{4}\right)\cdot\left(\frac{2}{2}:\frac{1}{1}-\frac{3}{3}:\frac{5}{1}\right)-\left(\frac{1}{1}:\frac{2}{3}+\frac{1}{1}-\frac{4}{3}\right)-\left(\frac{5}{4}\cdot\frac{1}{5}:\frac{3}{4}+\frac{4}{2}:\frac{4}{3}\cdot\frac{2}{2}\right)$$

Rozszyfruj zakodowany tekst. Przetłumacz cytat na język polski.

Wykonaj działania na wskazanych ułamkach stosując odpowiednie reguły matematyczne. Wynik zapisz w postaci nieskracalnego ułamka zwykłego.

ZAD.3. (12 pkt.)

Szyfr Vigenère jest szyfrem przestawieniowym polialfabetycznym, którego tekst jawny jest szyfrowany na podstawie klucza oraz tabelki. Tabelka jest stała i reprezentuje ją 26 liter (w przypadku alfabetu łacińskiego).

	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

Tabelka jest bardzo duża, ale bardzo łatwo ją zapamiętać, ponieważ alfabet znajdujący się w *i*-tym wierszu jest alfabetem przesuniętym w lewo o *i - 1* pozycji.

Przykład
Szyfrując wyraz **INFORMACJA** kluczem **HASLO** należy kolejno: dla litery **I** odczytać wartość z kolumny **I** i wiersza **H**. W tym przypadku jest to litera **P**. Dla kolejnej litery będzie to kolumna **N** i wiersz **A**. W przypadku litery **A** żadna litera nie zostaje zaszyfrowana, ponieważ alfabet dla litery **A** klucza alfabet ma przesunięcie 0. Ostatecznie zaszyfrowany tekst to: **PNXZFTAUUO**.

Podczas deszyfrowania szyfrogramu **PNXZFTAUUO** przy pomocy klucza **HASLO** należy pamiętać, że: pierwsza litera szyfrogramu to **P**. W kolumnie **H** należy znaleźć wartość **P** i odczytać nagłówek wiersza. **P** zostaje rozszyfrowane jako **I**. Kontynuując w ten sposób uzyska się tekst jawny **INFORMACJA**.

Poniższy tekst zaszyfrowano korzystając z szyfru polialfabetycznego z wykorzystaniem kwadratu Vigenere'a. Do szyfrowania użyto słowa klucza.

Rozwiąż krzyżówkę. Wypisz litery z pól zaznaczonych w krzyżówce. Słowo kluczowe jest 7-literowym anagramem o początkowej literze K, utworzonym z tych liczb.

Wykorzystując macierz Vigenere'a oraz słowo kluczowe rozszyfruj następującą wiadomość:

UFLZNFYBOSSU KG CNGEER HBNRUMQLKZPKHZS DSXCNL
RBCMEGZSV STY XCS GGMIMKCSQU G NVCCH MKMQQPFBGUEQ

Podaj pełne rozwiązanie zadania tzn. wypełnioną krzyżówkę [każde hasło], słowo klucz, rozszyfrowany tekst z pełnym uzasadnieniem sposobu deszyfrowania poszczególnych słów.

KRZYŻÓWKA NA NASTĘPNEJ STRONIE