ZAKRES MATERIAŁU

I. Definicja systemu kryptograficznego

- **tekst jawny** - informacja (komunikat), którą chcemy przekazać przez niechroniony kanał,
- **kryptogram** (tekst zaszyfrowany)

[DEF 01] (system kryptograficzny (kryptosystem))
– dowolna piątka (P, C, K, E, D) spełniająca cztery warunki

(1) P – skończony zbiór możliwych tekstów jawnych (zbiór komunikatów),
(2) C – skończony zbiór możliwych tekstów zaszyfrowanych (zbiór kryptogramów),
(3) K – skończony zbiór możliwych kluczy,
(4) $\forall_{x\in P}\ \forall_{K\in K}\ \exists_{\substack{e_K\in E\\ d_K\in D}}\ d_k(e_k(x)) = x$

- $e_K \in E$ - reguła szyfrowania (funkcja $e_K : P \to C$),
- $d_K \in D$ - regułą deszyfrowania odpowiadająca regule szyfrowania $e_K \in E$ (funkcja $d_K : C \to P$),

---

[Umowa] Do proponowanych szyfrów stosujemy tu pierścień Z_{26} ze względu na liczność zbioru liter alfabetu angielskiego. W ogólnym przypadku można jednak użyć dowolnego pierścienia Z_m.

II. Szyfr z przesunięciem (szyfr Cezara)

[Algorytm] (**szyfr z przesunięciem** (**szyfr Cezara**) (szyfr oparty na arytmetyce reszt))
Niech $P = C = K = Z_{26}$.
Dla $0 \le K \le 25$ definiujemy

- regułę szyfrowania $e_K(x) = (x + K) \bmod 26$
- regułę deszyfrowania $d_K(y) = (y - K) \bmod 26$

gdzie $x, y \in Z_{26}$.
Dla szyfru Cezara istnieje tylko 26 możliwych kluczy.

[Zadanie 01] Zrealizuj szyfrowanie i deszyfrowanie tekstu T za pomocą szyfru Cezara.
Dane:
klucz K = 11
tekst otwarty T = kryptografia

Odpowiedniość między znakami alfabetu a resztami modulo 26.

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
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

T = k r y p t o g r a f i a

- SZYFROWANIE

(1) przekształcamy tekst T zgodnie z tabelką odpowiedniości między znakami a resztami modulo 26.
10 17 24 15 19 14 6 17 0 5 8 0
(2) dodajemy do każdej z wartości K=11
21 28 35 26 30 25 17 28 11 16 19 11
(3) redukujemy powyższe wartości modulo 26
21 2 9 0 4 25 17 2 11 16 19 11
(4) ostateczny zaszyfrowany tekst otrzymujemy przekształcając powyższy ciąg liczb w znaki alfabetu
VCJAEZRCLQTL

- DESZYFROWANIE

(1) przekształcamy zaszyfrowany tekst w ciąg liczb
(2) od każdej z liczb odejmujemy K=11
(3) redukujemy otrzymane wartości modulo 26
(4) otrzymany ciąg liczb zamieniamy w ciąg liter zgodnie z tabelką odpowiedniości

---

III. Monoalfabetyczny szyfr podstawieniowy

[Algorytm] (**monoalfabetyczny**[(1)] **szyfr podstawieniowy**)
Niech $P = C = Z_{26}$, K – zbiór wszystkich permutacji liczb 0, 1, ..., 25.
Dla zadanej permutacji $\pi \in K$ definiujemy funkcje: szyfrującą i deszyfrującą

- $e_\pi(x) = \pi(x)$
- $d_\pi(y) = \pi^{-1}(y)$,

gdzie π^{-1} jest permutacją odwrotną do π.
Kluczem do szyfru podstawieniowego jest permutacja 26 znaków. Takich kluczy jest 26!.

[Zadanie 02] Zaszyfruj podany tekst T metodą podstawieniową z funkcją szyfrującą $e_\pi(x) = \pi(x)$ zadaną poniższą tabelką.
Dane:
Tekst otwarty T = kryptografia

$e_\pi(x) = \pi(x)$ funkcja szyfrująca

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

np. $e_\pi(a) = F$

$d_\pi(y) = \pi^{-1}(y)$ funkcja deszyfrująca

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
g	k	o	s	w	a	d	i	m	q	t	x	z	b	e	h	l	P	r	u	y	f	c	j	n	v

np. $d_\pi(A) = g$

Zaszyfrowany tekst (kryptogram) to BSURKCASFVHF

([1]) **szyfr monoalfabetyczny** - szyfr, w którym jednej literze alfabetu jawnego odpowiada dokładnie jedna litera alfabetu tajnego

IV. Szyfr Vigenere'a

[Algorytm] (szyfr Vigenere'a)

Niech $n \in Z_+$ będzie ustalone oraz niech $P = C = K = (Z_{26})^n$.

Dla klucza $K = (k_1,...,k_n)$ definiujemy funkcję szyfrującą i deszyfrującą

- $e_K(x_1, x_2,..., x_n) = (x_1 + k_1, x_2 + k_2,..., x_n + k_n)$ i
- $d_K(y_1, y_2,..., y_n) = (y_1 - k_1, y_2 - k_2,..., y_n - k_n)$

Wszystkie działania arytmetyczne wykonywane są w Z_{26}.
Szyfr Vigenere'a jest przykładem polialfabetycznego[2] szyfru podstawieniowego.

[Zadanie 03] Zaszyfruj podany tekst T metodą Vigenere'a.
Dane:
n=6,
słowo kluczowe K = KARTON
jego liczbowy odpowiednik to K = (10, 0, 17, 19, 14, 13)
T = kryptografia

T = k r y p t o g r a f i a

- SZYFROWANIE

(1) przekształcamy symbole tekstu jawnego w reszty modulo 26
10 17 24 15 19 14 6 17 0 5 8 0
(2) zapisujemy je w grupach po n=6 i dodajemy słowo kluczowe K modulo 26
10 17 24 15 19 14 6 17 0 5 8 0
10 0 17 19 14 13 10 0 17 19 14 13
---
20 17 15 8 7 1 16 17 17 24 22 13
(3) otrzymany ciąg liczb zamieniamy w ciąg liter zgodnie z tabelką odpowiedniości
URPIHBQRRYWN

- DESZYFROWANIE

(1) przekształcamy symbole tekstu jawnego w reszty modulo 26
20 17 15 8 7 1 16 17 17 24 22 13
(2) zapisujemy je w grupach po n=6 i odejmujemy słowo kluczowe modulo 26
20 17 15 8 7 1 16 17 17 24 22 13
10 0 17 19 14 13 10 0 17 19 14 13
---
10 17 24 15 19 14 6 17 0 5 8 0
(3) otrzymany ciąg liczb zamieniamy w ciąg liter zgodnie z tabelką odpowiedniości

---

V. Szyfr przestawieniowy (permutacyjny)

[Idea] Znaki tekstu jawnego pozostają niezmienione, zmienia się jedynie ich kolejność.

[Algorytm] (Szyfr przestawieniowy (permutacyjny))

Niech $n \in Z_+$ będzie ustalone oraz niech $P = C = (Z_{26})^n$ i

niech K będzie zbiorem wszystkich permutacji zbioru {1, 2, ..., n}.
Dla klucza (czyli permutacji) π definiujemy funkcję szyfrującą i deszyfrującą

- $e_\pi(x_1, x_2,..., x_n) = (x_{\pi(1)}, x_{\pi(2)},..., x_{\pi(n)})$ i
- $d_K(y_1, y_2,..., y_n) = (y_{\pi^{-1}(1)}, y_{\pi^{-1}(2)},..., y_{\pi^{-1}(n)})$

gdzie π^{-1} jest permutacją odwrotną do π.

[Zadanie 04] Zaszyfruj podany tekst T szyfrem permutacyjnym. Niepełny n-ciąg uzupełnij znakami 'x'.
Dane:
n=6
T = kryptografia
klucz: permutacja π postaci:
1 2 3 4 5 6
3 5 1 6 4 2
permutacja odwrotna π^{-1}:
1 2 3 4 5 6
3 6 1 5 2 4

T = k r y p t o g r a f i a

- SZYFROWANIE

(1) dzielimy tekst na grupy sześcioliterowe (ostatni niepełny ciąg możemy dopełnić np. znakami 'x')
krypto grafia
(2) w każdej z grup przestawiamy litery zgodnie z permutacją π
ytkopr aigafr
(3) uzyskany tekst zaszyfrowany to YTKOPRAIGAFR

- DESZYFROWANIE

Przy deszyfrowaniu stosujemy permutację π^{-1}.

[Zadanie 05] Wygeneruj permutacje odwrotne do podanych.
(a) π = (62457183) (b) EMBED Equation.3 π = (bhdfacge) (c) EMBED Equation.3
π = (EBJDAHFCIG)

(a) $\pi^{-1} = \begin{pmatrix} 1&2&3&4&5&6&7&8 \\ 6&2&4&5&7&1&8&3 \end{pmatrix}^{-1} = \begin{pmatrix} 6&2&4&5&7&1&8&3 \\ 1&2&3&4&5&6&7&8 \end{pmatrix} = \begin{pmatrix} 1&2&3&4&5&6&7&8 \\ 6&2&8&3&4&1&5&7 \end{pmatrix}$

(b) $\pi^{-1} = \begin{pmatrix} a&b&c&d&e&f&g&h \\ b&h&d&f&a&c&g&e \end{pmatrix}^{-1} = \begin{pmatrix} b&h&d&f&a&c&g&e \\ a&b&c&d&e&f&g&h \end{pmatrix} = \begin{pmatrix} a&b&c&d&e&f&g&h \\ e&a&f&c&h&d&g&b \end{pmatrix}$

[Zadanie 06] Uzupełnij ciało każdej z metod klas Cezar, podst_mono i Vigenere tak, aby klasy te realizowały szyfrowanie i deszyfrowanie w przedstawionych wyżej systemach. Następnie zrealizuj zapisany poniżej kod.

[2] **szyfr polialfabetyczny** - system kryptograficzny, w którym dowolny znak alfabetu może być przekształcony na jeden z m możliwych znaków (przy założeniu, że słowo kluczowe ma m znaków i wszystkie te znaki są różne). SP składa się z m przekształceń, takich że pierwszą literę szyfrujemy pierwszym przekształceniem, drugą – drugim, ..., m+1-szą – pierwszym itd.

KAPITAŁ LUDZKI NARODOWA STRATEGIA SPÓJNOŚCI
UNIA EUROPEJSKA EUROPEJSKI FUNDUSZ SPOŁECZNY
Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

```
szyfr Cezara
class cezar{
private String alf="";//alfabet
private int K;        //klucz
public cezar(String alf, int K){…}
//szyfrowanie
public String szyfr(String s){…}
//deszyfrowanie
public String deszyfr(String s){…}
//reguła szyfrowania
private int e_K(int a){…}
//reguła deszyfrowania
private int d_K(int a){…}
public String toString(){
return "----------\nszyfr Cezara\nalfabet="+alf+"\nklucz="+K;}
}
//-------------------------------------------------------------
//monoalfabetyczny szyfr podstawieniowy
class podst_mono{
private String alf="";//alfabet
private String K="";  //klucz
private String K1=""; //permutacja odwrotna do K
public podst_mono(String alf, String K){…}
//tworzy permutację odwrotną do s
private String permOdwr(String s){…}
//szyfrowanie
public String szyfr(String s){…}
//deszyfrowanie
public String deszyfr(String s){…}
//reguła szyfrowania
private char e_K(char a){…}
//reguła deszyfrowania
private char d_K(char a){…}
public String toString(){
return "----------\nmonoalfabetyczny szyfr podstaw.\nalfabet="+alf+"\nklucz="+K+
       "\npermutacja odwrotna K1="+K1;}
}
//-------------------------------------------------------------
//szyfr Vigenere'a
class Vigenere{
private String alf="";//alfabet
private String K;     //klucz
public Vigenere(String alf, String K){…}
//szyfrowanie
public String szyfr(String s){…}
//deszyfrowanie
public String deszyfr(String s){…}
//reguła szyfrowania
private String e_K(String x){…}
//reguła deszyfrowania
private String d_K(String y){…}
public String toString(){…}
return "----------\nszyfr Vigenere'a\nalfabet="+alf+"\nklucz="+K;}
}
//-------------------------------------------------------------
public class PS01{

  public static void main(String[] args){

  cezar sys01 = new cezar("abcdefghijklmnopqrstuvwxyz",11);
  System.out.println(sys01);
  System.out.println(sys01.szyfr("kryptografia"));
  System.out.println(sys01.deszyfr(sys01.szyfr("kryptografia")));

  podst_mono sys02 = new podst_mono("abcdefghijklmnopqrstuvwxyz","fnwgovaphxbqiycrjsdktzelum");
  System.out.println(sys02);
  System.out.println(sys02.szyfr("kryptografia"));
  System.out.println(sys02.deszyfr(sys02.szyfr("kryptografia")));

  Vigenere sys03 = new Vigenere("abcdefghijklmnopqrstuvwxyz","kreda");
  System.out.println(sys03);
  System.out.println(sys03.szyfr("kryptografia"));
  System.out.println(sys03.deszyfr(sys03.szyfr("kryptografia")));
  }
}
//-------------------------------------------------------------
```

REALIZACJA

```
//-------------------------------------------------------------
----------
szyfr Cezara
alfabet=abcdefghijklmnopqrstuvwxyz
klucz=11
vcjaezrclqtl
kryptografia
----------
monoalfabetyczny szyfr podstaw.
alfabet=abcdefghijklmnopqrstuvwxyz
klucz=fnwgovaphxbqiycrjsdktzelum
permutacja odwrotna K1=gkoswadimqtxzbehlpruyfcjnv
bsurkcasfvhf
kryptografia
----------
szyfr Vigenere'a
alfabet=abcdefghijklmnopqrstuvwxyz
klucz=kreda
uicstyxvdfsr
kryptografia
//-------------------------------------------------------------
```


KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI
UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY
Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego