-KOLO A ----------

[1] Wykonaj poniższe operacje w arytmetyce (mod m). Podaj rozwiązanie w zbiorze {0, 1, ..., m-1}.
(a) $141^{314}*15^{41} \pmod{281}$,
(b) $x \equiv (16^4 - 32^3) \bmod 41$.

---

[2] Znajdź wszystkie rozwiązania poniższej kongruencji w zbiorze {0, 1, ..., m-1} dla modułu m. Skorzystaj z twierdzenia 03.
$3x \equiv 4 \pmod{12}$

[TW03] Weźmy kongruencję liniową $ax \equiv b \pmod{m}$. Załóżmy (bez straty ogólności), że $0 \le a, b<m$).

- jeśli $NWD(a,m) = 1$, to jej rozwiązanie x_0 łatwo znaleźć Wszystkie inne rozwiązania mają postać $x = x_0 + mn$ dla $n \in Z$.
- jeśli $NWD(a,m) = d$, to jej rozwiązanie istnieje wtw d|b.
  W tym przypadku jest ona równoważna (ma takie same rozwiązania) jak kongruencja $a'x \equiv b' \pmod{m'}$, gdzie $a' = a/d$, $b' = b/d$, $m' = m/d$.

---

[3] Dla zadanej macierzy wyznacz ręcznie
(a) wyznacznik macierzy,
(b) macierz dopełnień algebraicznych,
(c) macierz dołączoną,
(d) macierz odwrotną.

$$A = \begin{bmatrix} 3 & 4 & 4 \\ 4 & 2 & 3 \\ 5 & 6 & 4 \end{bmatrix}$$

---

[4] Poniższy kryptogram uzyskano stosując szyfr Vigenere'a. Metodą Kasiskiego wyznaczono (prawdopodobną) długość klucza m=6. Podaj 6 podciągów poniższego ciągu znaków, dla których wskaźniki koincydencji (wyznaczane w metodzie Friedmana) będą (prawdopodobnie) najbardziej zbliżone do wartości 0,065. Zaszyfrowano tekst angielski.
"dfwkogusfuwvrwadzsqalfywckgeeivzxleckldtkiig"

---

[5] Wyznacz wzajemny indeks zgodności dla poniższych ciągów znaków.
s1="abcdedaebceadb"
s2="adfecberdcab"

---

[6] Kody Huffmana.
(a) Wygeneruj drzewo kodów Huffmana do zakodowania poniżej podanego tekstu (Uwzględnij spacje),
(b) Przypisz kody znakom znajdującym się w liściach drzewa Huffmana,
(c) Zakoduj podany tekst przy pomocy wyznaczonych kodów Huffmana.
"krolowa karolina",

---

[7] Wygeneruj klucz publiczny i prywatny w systemie RSA dla poniższych danych. Jeśli wartości p i q nie spełniają narzucanych na nie warunków, uzasadnij dlaczego.
p=13, q=101,

---

[8] Zapisz liczbę c w systemie pozycyjnym o zadanej podstawie.
$135 = (.....)_4$,

---

[9] Wyznacz wartość symbolu Jacobiego $\left(\frac{441}{1113}\right)$. Zapisz numery własności, z których kolejno korzystałeś.

---

[10] Podaj kryptogram dla tekstu otwartego "kartoteka" utajnionego przy pomocy szyfru permutacyjnego. Dla sprawdzenia zapisz odszyfrowany kryptogram. Przyjmij następujące założenia.
- znaki alfabetu angielskiego utożsam z liczbami z zakresu [0,...,25],
- za klucz przyjmij następujący łańcuch znaków: "513264".

ROZWIĄZANIE
Rozwiązanie:
[1] (a) $141^{314}*15^{41} \pmod{281}$, $141^{314} \pmod{281}=279$, $15^{41} \pmod{281}=42$, $279*42 \pmod{281}=197$,
(b) $(16^4-32^3) \bmod 41$, $16^4 \pmod{41}=18$, $32^3 \pmod{41}=9$, $(18-9) \bmod 41=9$,

---

[2] $NWD(3,12)=3$ i $3 \nmid 4$, więc na mocy tw03 kongruencja nie ma rozwiązań.

---

[3] (a) detA=22,

(b) $adjA = \begin{bmatrix} -10 & -1 & 14 \\ 8 & -8 & 2 \\ 4 & 7 & -10 \end{bmatrix}$ (c) $(adjA)^T = \begin{bmatrix} -10 & 8 & 4 \\ -1 & -8 & 7 \\ 14 & 2 & -10 \end{bmatrix}$

(d) $A^{-1} = (\det A)^{-1} * (adjA)^T = 22^{-1} * \begin{bmatrix} -10 & 8 & 4 \\ -1 & -8 & 7 \\ 14 & 2 & -10 \end{bmatrix} = \begin{bmatrix} \frac{-10}{22} & \frac{8}{22} & \frac{4}{22} \\ \frac{-1}{22} & \frac{-8}{22} & \frac{7}{22} \\ \frac{14}{22} & \frac{2}{22} & \frac{-10}{22} \end{bmatrix} =$

$$= \begin{vmatrix} -0.454545, & 0.363636, & 0.181818 \\ -0.045455, & -0.363636, & 0.318182 \\ 0.636364, & 0.090909, & -0.454545 \end{vmatrix}$$

---

[4]
s0=durqcvki
s1=fswakzlg
s2=wfalgxd
s3=kudfelt
s4=owzyeek
s5=gvswici

---

[5] Wzajemny indeks zgodności $MI_C(x,y) = \frac{\sum_{i=0}^{25} f_i f_i'}{nn'}$.

s1="abcdedaebceadb" n=14,
tablica f częstości wystąpień znaków alfabetu angielskiego w tekście s1
a b c d e f r
3,3,2,3,3,0,0,
s2="adfecberdcab" n'=12,
tablica f' częstości wystąpień znaków alfabetu angielskiego w tekście s2

a b c d e f r
2,2,2,2,2,1,1

$MI_C(sl, s2) = 0.16666666666666667,$

---

[6] (a)
lista:
_-0.0625, i-0.0625, n-0.0625, w-0.0625, k-0.125, l-0.125, r-0.125,
a-0.1875, o-0.1875,
drzewo w porządku KLP:
<KLP>: _-1.0, _-0.4375, o-0.1875, _-0.25, k-0.125, l-0.125, _-0.5625, _-0.25,
r-0.125, _-0.125, -0.0625, i-0.0625, _-0.3125, _-0.125, n-0.0625, w-0.0625,
a-0.1875,
kody:
spacja=1010, o=00, i=1011, k=010, w=1101, a=111, r=100, n=1100, l=011,
0101000001100110111110100101111000001110111100111

---

[7] RSA. p=13, q=101, n=1313, a=343, b=7,

---

[8] $135=(2,0,1,3)_4$,

--

[9] (441/1113)=
= (1113/441) z(3)
= (231/441), z(4)
= (441/231) z(3)
= (210/231), z(4)
= (105/231), z(5)
= (231/105) z(3)
= (21/105), z(4)
= (105/21) z(3)
= (0/21), z(4)
=0, (def s. Legendre'a)

---

[10] permutacja ”513264”, permutacja odwrotna ”243615”
szyfrogram - ”okrattxeakxx”
po deszyfrowaniu - ”kartotekaxxx”

-KOLO B----------

[1] Wygeneruj klucz publiczny i prywatny w systemie RSA dla poniższych danych. Jeśli wartości p i q nie spełniają narzucanych na nie warunków, uzasadnij dlaczego.
p=17, q=71,

---

[2] Znajdź wszystkie rozwiązania poniższej kongruencji w zbiorze {0, 1, ..., m-1} dla modułu m. Skorzystaj z twierdzenia 02.
$103x \equiv 612 (\mathrm{mod}\, 676)$

[TW02] Weźmy kongruencję liniową $ax \equiv b (\mathrm{mod}\, m)$. Załóżmy (bez straty ogólności), że $0 \leq a$, b<m).

- jeśli $NWD(a, m) = 1$, to jej rozwiązanie x_0 łatwo znaleźć Wszystkie inne rozwiązania mają postać $x = x_0 + mn$ dla $n \in Z$.
- jeśli $NWD(a, m) = d$, to jej rozwiązanie istnieje wtw d|b.

  W tym przypadku jest ona równoważna (ma takie same rozwiązania) jak kongruencja $a'x \equiv b' (\mathrm{mod}\, m')$, gdzie $a' = a/d$, $b' = b/d$, $m' = m/d$.

---

[3] Poniższy kryptogram uzyskano stosując szyfr Vigenere'a. Metodą Kasiskiego wyznaczono (prawdopodobną) długość klucza m=4. Podaj 4 podciągi poniższego ciągu znaków, dla których wskaźniki koincydencji (wyznaczane w metodzie Friedmana) będą (prawdopodobnie) najbardziej zbliżone do wartości 0,065. Zaszyfrowano tekst angielski.
”dfwkogusfuwvrwadzsqalfywckgeeivzxleckldtkiig”

---

[4] Wykonaj poniższe operacje w arytmetyce (mod m). Podaj rozwiązanie w zbiorze {0, 1, ..., m-1}.
(a) $131^{116} * 16^{41} (\mathrm{mod}\, 381)$,
(b) $x \equiv (16^3 + 52^3) \bmod 41$.

---

[5] Wyznacz wzajemny indeks zgodności dla poniższych ciągów znaków.
s1=”dceabcdedaebce”
s2=”adfecbercded”

---

[6] Kody Huffmana.
(a) Wygeneruj drzewo kodów Huffmana do zakodowania poniżej podanego tekstu (Uwzględnij spacje),
(b) Przypisz kody znakom znajdującym się w liściach drzewa Huffmana,
(c) Zakoduj podany tekst przy pomocy wyznaczonych kodów Huffmana.
”kolorowy koralik”,

---

[7] Zapisz liczbę c w systemie pozycyjnym o zadanej podstawie.
$145 = (.....)_3$,

---

[8] Wyznacz wartość symbolu Jacobiego $\left(\frac{411}{1317}\right)$. Zapisz numery własności, z których kolejno korzystałeś.

---

[9] Podaj kryptogram dla tekstu otwartego ”kryptografia” utajnionego przy pomocy szyfru permutacyjnego. Dla sprawdzenia zapisz odszyfrowany kryptogram. Przyjmij następujące założenia.
- znaki alfabetu angielskiego utożsam z liczbami z zakresu [0,...,25],
- za klucz przyjmij następujący łańcuch znaków: ”451326”.

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

---

[10] Dla zadanej macierzy wyznacz ręcznie
(a) wyznacznik macierzy,
(b) macierz dopełnień algebraicznych,
(c) macierz dołączoną,
(d) macierz odwrotną.

$$A = \begin{bmatrix} 1 & 4 & 4 \\ 4 & 2 & 3 \\ 6 & 6 & 4 \end{bmatrix}$$

ROZWIĄZANIE

[1] p=17, q=71, n=1207, a=747, b=3,

---

[2] NWD(103,676)=1, 103*x = 676*636+612 dla x=96,

---

[3] s0=dofrzlcexkk
s1=fguwsfkilli
s2=wuwaqygvedi
s3=ksvdawezctg

---

[4] (a) $131^{116}*16^{41}$(mod 381), 131^{116}(mod 381)=256, 16^{41}(mod 381)=262, 256*262(mod 381)=16,
(b) (16^3+52^3)mod 41, 16^3mod 41=37, 52^3mod 41=19, (37+19)mod 41=15,

---

[5] Wzajemny indeks zgodności $MI_C(x,y) = \frac{\sum_{i=0}^{25} f_i f_i'}{nn'}$.

s1=”dceabcdedaebce” n=14,
tablica f częstości wystąpień znaków alfabetu angielskiego w tekście s1
a b c d e f r
2,2,3,3,4,0,0
s2=”adfecbercded” n’=12,
tablica f’ częstości wystąpień znaków alfabetu angielskiego w tekście s2
a b c d e f r
1,1,2,3,3,1,1
$MI_C(s1,s2)$ = 0.18452380952380953,

---

[6] lista:
spacja-0.0625, a-0.0625, i-0.0625, w-0.0625, y-0.0625, l-0.125, r-0.125,
k-0.1875, o-0.25,
drzewo Huffmana w porządku KLP:
_-1.0, _-0.4375, _-0.1875, y-0.0625, l-0.125, o-0.25, _-0.5625, _-0.25,
r-0.125, _-0.125, spacja-0.0625, a-0.0625, _-0.3125, _-0.125, i-0.0625,
w-0.0625, k-0.1875,
kody Huffmana:
spacja=1010, o=01, i=1100, k=111, w=1101, a=1011, r=100, y=000, l=001
zakodowany ciąg:
111010010110001110100010101110110010110011100111

---

[7] 145=$(1,2,1,0,1)_3$,

---

[8] (411/1317)=
= (1317/411),z(3)
= (84/411), z(4)
=-(42/411), z(5)
= (21/411), z(5)
= (411/21), z(3)
= (12/21), z(4)
=-(6/21), z(5)
= (3/21), z(5)
= (21/3), z(3)
= (0/3), z(4)
=0, (def s. Legendre'a)

[9] permutacja ”451326”, permutacja odwrotna ”354126”
szyfrogram - ”ptkyrofigara”
po deszyfrowaniu - ”kryptografia”

--

[10] (a) detA=46,

(b) $\text{adjA} = \begin{bmatrix} -10 & 2 & 12 \\ 8 & -20 & 18 \\ 4 & 13 & -14 \end{bmatrix}$

(c) $(\text{adjA})^T = \begin{bmatrix} -10 & 8 & 4 \\ 2 & -20 & 13 \\ 12 & 18 & -14 \end{bmatrix}$

(d) $A^{-1} = (\det A)^{-1} * (\text{adjA})^T = 46^{-1} * \begin{bmatrix} -10 & 8 & 4 \\ 2 & -20 & 13 \\ 12 & 18 & -14 \end{bmatrix} = \begin{bmatrix} \frac{-10}{46} & \frac{8}{46} & \frac{4}{46} \\ \frac{2}{46} & \frac{-20}{46} & \frac{13}{46} \\ \frac{12}{46} & \frac{18}{46} & \frac{-14}{46} \end{bmatrix} =$

|-0.217391, 0.173913, 0.086957|
=| 0.043478,-0.434783, 0.282609|
| 0.260870, 0.391304,-0.304348|

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

-KOLO C----------

[1] Wykonaj poniższe operacje w arytmetyce (mod m). Podaj rozwiązanie w zbiorze {0, 1, ..., m-1}.
(a) $131^{315}*35^{41} \pmod{211}$,
(b) $x \equiv (16^4 - 42^3) \bmod 43$.

---

[2] Dla zadanej macierzy w arytmetyce (mod 41) wyznacz
(a) wyznacznik macierzy,
(b) macierz dopełnień algebraicznych,
(c) macierz dołączoną,
(d) macierz odwrotną.

$$A = \begin{bmatrix} 1 & 3 & 2 & 3 \\ 2 & 6 & 3 & 11 \\ 3 & 4 & 8 & 20 \\ 1 & 21 & 12 & 8 \end{bmatrix}$$

---

[3] Kody Huffmana.
(a) Wygeneruj drzewo kodów Huffmana do zakodowania poniżej podanego tekstu (Uwzględnij spacje),
(b) Przypisz kody znakom znajdującym się w liściach drzewa Huffmana,
(c) Zakoduj podany tekst przy pomocy wyznaczonych kodów Huffmana.
”lampa alladyna”,

---

[4] Zapisz liczbę c w systemie pozycyjnym o zadanej podstawie.
$165=(.....)_6$,

---

[5] Wyznacz wzajemny indeks zgodności dla poniższych ciągów znaków.
s1=”cbcdadadebceadb”
s2=”cdfeccaddcab”

---

[6] Podaj kryptogram dla tekstu otwartego ”karkonosze” utajnionego przy pomocy szyfru permutacyjnego. Dla sprawdzenia zapisz odszyfrowany kryptogram. Przyjmij następujące założenia.
- znaki alfabetu angielskiego utożsam z liczbami z zakresu [0,...,25],
- za klucz przyjmij następujący łańcuch znaków: ”451326”.

---

[7] Znajdź wszystkie rozwiązania poniższej kongruencji w zbiorze {0, 1, ..., m-1} dla modułu m. Skorzystaj z twierdzenia 03.
$8x \equiv 4 \pmod{24}$

[TW03] Weźmy kongruencję liniową $ax \equiv b \pmod{m}$. Załóżmy (bez straty ogólności), że $0 \le a$, b<m).

- jeśli $NWD(a,m) = 1$, to jej rozwiązanie x_0 łatwo znaleźć Wszystkie inne rozwiązania mają postać $x = x_0 + mn$ dla $n \in Z$.
- jeśli $NWD(a,m) = d$, to jej rozwiązanie istnieje wtw d|b.

  W tym przypadku jest ona równoważna (ma takie same rozwiązania) jak kongruencja $a'x \equiv b' \pmod{m'}$, gdzie $a' = a/d$, $b' = b/d$, $m' = m/d$.

---

[8] Wyznacz z definicji wartość symbolu Legendre’a $\left(\frac{4}{23}\right)$.

---

[9] Podaj zbiór dodatnich reszt kwadratowych dla modułu p=101.

---

[10] System RSA jako szyfr blokowy. Dane są N-elementowy alfabet $\Sigma = \{0,1,...,N-1\}$ oraz wartości p, q. Ustal (dla szyfrowania) długość bloków tekstu jawnego. Jeśli dane nie spełniają narzucanych na nie warunków, uzasadnij dlaczego.
p=13, q=17, $\Sigma = \{0,1,...,31\}$,

ROZWIĄZANIE

[1] (a) $131^{315}*35^{41} \pmod{211}$, $131^{315} \pmod{211}=210$, $35^{41} \pmod{211}=202$, $210*202 \pmod{211}=9$,
(b) $16^4-42^3 \pmod{43}$, $16^4 \pmod{43}=4$, $42^3 \pmod{43}=42$, $4-42 \pmod{43}=5$,

---

[2] (a) detA=3,

(b) $adjA = \begin{bmatrix} 18 & 15 & 13 & 26 \\ 30 & 23 & 18 & 37 \\ 28 & 14 & 33 & 23 \\ 5 & 20 & 16 & 36 \end{bmatrix}$, (c) $(adjA)^T = \begin{bmatrix} 18 & 30 & 28 & 5 \\ 15 & 23 & 14 & 20 \\ 13 & 18 & 33 & 16 \\ 26 & 37 & 23 & 36 \end{bmatrix}$, (d) $A^{-1} = \begin{bmatrix} 6 & 10 & 23 & 29 \\ 5 & 35 & 32 & 34 \\ 18 & 6 & 11 & 19 \\ 36 & 26 & 35 & 12 \end{bmatrix}$

---

[3] lista:
spc-0.0714, d-0.0714, m-0.0714, n-0.0714, p-0.0714, y-0.0714, l-0.2143, a-0.3571,
drzewo w porządku KLP:
<KLP>: _-1.0, a-0.3571, _-0.6429, _-0.2857, _-0.1429, spc-0.0714, d-0.0714, _-0.1429, m-0.0714, n-0.0714, _-0.3571, _-0.1429, p-0.0714, y-0.0714, l-0.2143,
kody Huffmana:
d=1001, spc=1000, m=1010, a=0, y=1101, p=1100, n=1011, l=111,
zakodowany tekst:
111010101100010000111111010011101101l0

---

[4] $165=(433)_6$,

---

[5] Wzajemny indeks zgodności $MI_C(x,y) = \frac{\sum_{i=0}^{25} f_i f_i'}{nn'}$.

s1=”cbcdadadebceadb”, n=15,
tablica f częstości wystąpień znaków alfabetu angielskiego w tekście s1

a	b	c	d	e	f
3	3	3	4	2	0

s2=”cdfeccaddcab” n’=12,
tablica f’ częstości wystąpień znaków alfabetu angielskiego w tekście s2

a	b	c	d	e	f
2	1	4	3	1	1

$MI_C(s1,s2) = 0.1944444444$,

---

[6] permutacja ” 451326”, permutacja odwrotna ”354126”
szyfrogram - ”kokranexozsx”, po deszyfrowaniu - ”karkonoszexx”

---

[7] NWD(8,24)=8 i $8 \nmid 4$, więc na mocy tw03 kongruencja nie ma rozwiązań.

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

[8] $\left(\frac{4}{23}\right) = 1$, ponieważ 4 jest resztą kwadratową (mod 23),

---

[9] Zbiór dodatnich reszt kwadratowych dla modułu p=101:
{1,4,5,6,9,13,14,16,17,19,20,21,22,23,24,25,30,31,33,36,37,43,45,47,49,
52,54,56,58,64,65,68,70,71,76,77,78,79,80,81,82,84,85,87,88,92,95,96,97,100}

---

[10] RSA. p=13, q=17, n=221, a=77, b=5, k=1,

-KOLO D----------

[1] Kody Huffmana.
(a) Wygeneruj drzewo kodów Huffmana do zakodowania poniżej podanego tekstu (Uwzględnij spacje),
(b) Przypisz kody znakom znajdującym się w liściach drzewa Huffmana,
(c) Zakoduj podany tekst przy pomocy wyznaczonych kodów Huffmana.
"kodowanie huffmana",

---

[2] Wyznacz wzajemny indeks zgodności dla poniższych ciągów znaków.
s1="bcdcbadebceadb"
s2="abdcdfeccadd"

---

[3] Podaj kryptogram dla tekstu otwartego "czekoladki" utajnionego przy pomocy szyfru permutacyjnego. Dla sprawdzenia zapisz odszyfrowany kryptogram. Przyjmij następujące założenia.
- znaki alfabetu angielskiego utożsam z liczbami z zakresu [0,...,25],
- za klucz przyjmij następujący łańcuch znaków: "645132".

---

[4] Wykonaj poniższe operacje w arytmetyce (mod m). Podaj rozwiązanie w zbiorze {0, 1, ..., m-1}.
(a) $151^{318} * 36^{46} \pmod{311}$,
(b) $x \equiv (16^4 - 41^3) \bmod 44$.

---

[5] Zapisz liczbę c w systemie pozycyjnym o zadanej podstawie.
$185 = (.....)_8$,

---

[6] Znajdź wszystkie rozwiązania poniższej kongruencji w zbiorze {0, 1, ..., m-1} dla modułu m. Skorzystaj z twierdzenia 03.
$8x \equiv 4 \pmod{32}$

[TW03] Weźmy kongruencję liniową $ax \equiv b \pmod{m}$. Załóżmy (bez straty ogólności), że $0 \le a, b < m$).
- jeśli $NWD(a,m) = 1$, to jej rozwiązanie x_0 łatwo znaleźć Wszystkie inne rozwiązania mają postać $x = x_0 + mn$ dla $n \in Z$.
- jeśli $NWD(a,m) = d$, to jej rozwiązanie istnieje wtw d|b.

W tym przypadku jest ona równoważna (ma takie same rozwiązania) jak kongruencja $a'x \equiv b' \pmod{m'}$, gdzie $a' = a/d$, $b' = b/d$, $m' = m/d$.

---

[7] Wyznacz z definicji wartość symbolu Legendre'a $\left(\frac{4}{71}\right)$.

---

[8] Podaj zbiór dodatnich reszt kwadratowych dla modułu p=103.

---

[9] Dla zadanej macierzy w arytmetyce (mod 32) wyznacz
(a) wyznacznik macierzy,
(b) macierz dopełnień algebraicznych,
(c) macierz dołączoną,
(d) macierz odwrotną.

$$A = \begin{bmatrix} 1 & 3 & 2 & 3 \\ 2 & 6 & 3 & 11 \\ 3 & 4 & 8 & 20 \\ 1 & 21 & 12 & 8 \end{bmatrix}$$

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

[10] System RSA jako szyfr blokowy. Dane są N-elementowy alfabet $\Sigma = \{0,1,...,N-1\}$ oraz wartości p, q. Ustal (dla szyfrowania) długość bloków tekstu jawnego. Jeśli dane nie spełniają narzucanych na nie warunków, uzasadnij dlaczego.
p=17, q=11, $\Sigma = \{0,1,...,26\}$,

ROZWIĄZANIE
[1] lista:
spc-0.0556, d-0.0556, e-0.0556, h-0.0556, i-0.0556, k-0.0556, m-0.0556,
u-0.0556, w-0.0556, f-0.1111, n-0.1111, o-0.1111, a-0.1667,
drzewo w porządku KLP:
_-1.0, _-0.4444, _-0.2222, n-0.1111, o-0.1111, _-0.2222, _-0.1111, spc-0.0556,
d-0.0556, _-0.1111, e-0.0556, h-0.0556, _-0.5556, _-0.2222, _-0.1111,
i-0.0556, k-0.0556, _-0.1111, m-0.0556, u-0.0556, _-0.3333, a-0.1667,
_-0.1667, w-0.0556, f-0.1111,
kody Huffmana:
o=001, d=0101, k=1001, w=1110, h=0111, spc=0100, i=1000, m=1010, a=110,
u=1011, f=1111, n=000, e=0110
zakodowany tekst:
1001001010100111101100001000011001000111101111111111110101100000110
---

[2] Wzajemny indeks zgodności $MI_C(x,y) = \frac{\sum_{i=0}^{25} f_i f_i'}{nn'}$.
s1="bcdcbadebceadb", n=14,
tablica f częstości wystąpień znaków alfabetu angielskiego w tekście s1 a b c d e f
2,4,3,3,2,0
s2="abdcdfeccadd" n'=12,
tablica f' częstości wystąpień znaków alfabetu angielskiego w tekście s2 a b c d e f
2,1,3,4,1,1
$MI_C(s1,s2) =$ 0.184523809,
---

[3] permutacja "645132", permutacja odwrotna "465231"
szyfrogram - "lkocezxixakd", po deszyfrowaniu - "czekoladkixx"
---

[4] (a) $151^{318} \pmod{311} = 125$, $36^{46} \pmod{311} = 36$, $125 * 36 \pmod{311} = 146$,
(b) $16^4 \pmod{44} = 20$, $41^3 \pmod{44} = 17$, $(20-17) \bmod 44 = 3$,
---

[5] $185 = (271)_8$,
---

[6] NWD(8,32)=8 i $8 \nmid 4$, więc na mocy tw03 kongruencja nie ma rozwiązań.
---

[7] $\left(\frac{4}{71}\right) = 1$, ponieważ 4 jest resztą kwadratową (mod 71),
---

[8] Zbiór dodatnich reszt kwadratowych dla modułu p=103:
{1,2,4,7,8,9,13,14,15,16,17,18,19,23,25,26,28,29,30,32,33,34,36,38,41,46,49,
50,52,55,56,58,59,60,61,63,64,66,68,72,76,79,81,82,83,91,92,93,97,98,100}
---

[9] (a) detA=19,

(b) $adjA = \begin{bmatrix} 4 & 24 & 9 & 7 \\ 16 & 28 & 31 & 10 \\ 5 & 23 & 6 & 14 \\ 0 & 11 & 7 & 27 \end{bmatrix}$, (c) $(adjA)^T = \begin{bmatrix} 4 & 16 & 5 & 0 \\ 24 & 28 & 23 & 11 \\ 9 & 31 & 6 & 7 \\ 7 & 10 & 14 & 27 \end{bmatrix}$, (d) $A^{-1} = \begin{bmatrix} 12 & 16 & 7 & 0 \\ 8 & 20 & 13 & 9 \\ 19 & 5 & 2 & 29 \\ 29 & 14 & 26 & 25 \end{bmatrix}$

---

[10] RSA. p=17, q=11, n=187, a=107, b=3, k=1

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

-KOLO E----------

[1] Wykonaj poniższe operacje w arytmetyce (mod m). Podaj rozwiązanie w zbiorze {0, 1, ..., m-1}.
(a) $141^{415} * 36^{41} \pmod{231}$,
(b) $x \equiv (18^4 - 41^3) \bmod 43$.

---

[2] Dla zadanej macierzy w arytmetyce (mod 41) wyznacz
(a) wyznacznik macierzy,
(b) macierz dopełnień algebraicznych,
(c) macierz dołączoną,
(d) macierz odwrotną.

$$A = \begin{bmatrix} 3 & 3 & 5 \\ 2 & 9 & 6 \\ 6 & 5 & 5 \end{bmatrix}$$

---

[3] Kody Huffmana.
(a) Wygeneruj drzewo kodów Huffmana do zakodowania poniżej podanego tekstu (Uwzględnij spacje),
(b) Przypisz kody znakom znajdującym się w liściach drzewa Huffmana,
(c) Zakoduj podany tekst przy pomocy wyznaczonych kodów Huffmana.
"filatelista",

---

[4] Zapisz liczbę c w systemie pozycyjnym o zadanej podstawie.
$145 = (.....)_6$,

---

[5] Wyznacz wzajemny indeks zgodności dla poniższych ciągów znaków.
s1="cadaadadebceadb"
s2="cddadcaddcab"

---

[6] Znajdź najmniejsze rozwiązanie poniższej kongruencji w zbiorze {0, 1, ..., m-1} dla modułu m.
$27x \equiv 72 \pmod{900}$

---

[7] Podaj zbiór dodatnich reszt kwadratowych dla modułu p=113.

---

[8] Eksperyment polega na n-krotnym rzucie symetryczną kostką sześcienną. Zbiór możliwych wyników jednego rzutu to X={I, II, III, IV, V, VI}. Które z poniższych kodowań jest wolne od przedrostków. Dla kodowań nie spełniających tej własności podaj odpowiedni kontrprzykład.
p(I)=00, p(II)=01, p(III)=10, p(IV)=11, p(V)=001, p(VI)=010,

---

[9] System RSA jako szyfr blokowy. Dane są N-elementowy alfabet $\Sigma = \{0,1,...,N-1\}$ oraz wartości p, q. Ustal (dla szyfrowania) długość bloków tekstu jawnego. Jeśli dane nie spełniają narzucanych na nie warunków, uzasadnij dlaczego.
p=13, q=17, $\Sigma = \{0,1,...,38\}$,

[10] Wyznacz wartość symbolu Jacobiego $\left(\frac{1152}{1239}\right)$. Zapisz z jakich własności korzystałeś w kolejnych krokach.

-KOLO F----------

[1] Dla zadanej macierzy w arytmetyce (mod 41) wyznacz
(a) wyznacznik macierzy,
(b) macierz dopełnień algebraicznych,
(c) macierz dołączoną,
(d) macierz odwrotną.

$$A = \begin{bmatrix} 4 & 3 & 5 \\ 2 & 9 & 6 \\ 3 & 5 & 5 \end{bmatrix}$$

---

[2] Zapisz liczbę c w systemie pozycyjnym o zadanej podstawie.
$135 = (.....)_5$,

---

[3] Wyznacz wzajemny indeks zgodności dla poniższych ciągów znaków.
s1="acaadadebceadb"
s2="abaadcaddcab"

---

[4] Znajdź najmniejsze rozwiązanie poniższej kongruencji w zbiorze {0, 1, ..., m-1} dla modułu m.
$26x \equiv 13 \pmod{39}$

---

[5] Eksperyment polega na n-krotnym rzucie symetryczną kostką sześcienną. Zbiór możliwych wyników jednego rzutu to X={I, II, III, IV, V, VI}. Które z poniższych kodowań jest wolne od przedrostków. Dla kodowań nie spełniających tej własności podaj odpowiedni kontrprzykład.
h(I)=00, h(II)=001, h(III)=011, h(IV)=111, h(V)=101, h(VI)=010,

---

[6] System RSA jako szyfr blokowy. Dane są N-elementowy alfabet $\Sigma = \{0,1,...,N-1\}$ oraz wartości p, q. Ustal (dla szyfrowania) długość bloków tekstu jawnego. Jeśli dane nie spełniają narzucanych na nie warunków, uzasadnij dlaczego.
p=11, q=17, $\Sigma = \{0,1,...,28\}$,

[7] Wyznacz wartość symbolu Jacobiego $\left(\frac{1152}{1259}\right)$. Zapisz z jakich własności korzystałeś w kolejnych krokach.

---

[8] Wykonaj poniższe operacje w arytmetyce (mod m). Podaj rozwiązanie w zbiorze {0, 1, ..., m-1}.
(a) $41^{415} * 35^{41} \pmod{231}$,
(b) $x \equiv (18^{41} - 31^{31}) \bmod 43$.

---

[9] Kody Huffmana.
(a) Wygeneruj drzewo kodów Huffmana do zakodowania poniżej podanego tekstu (Uwzględnij spacje),
(b) Przypisz kody znakom znajdującym się w liściach drzewa Huffmana,
(c) Zakoduj podany tekst przy pomocy wyznaczonych kodów Huffmana.
"antropologia"

---

[10] Podaj zbiór dodatnich reszt kwadratowych dla modułu p=71.

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