Wstęp do matematyki - Mały projekt 1
Temat: Kryptografia symetryczna
Jan Czechowski

zad.1

In[9]:=
```
wiadomosc =
  LetterNumber["STUDIUJĘ CYBERBEZPIECZEŃSTWO BO LUBIĘ KRYPTOGRAFIĘ", "Polish"];
kluczK = RandomInteger[{0, 31}, Length[wiadomosc]];
```

In[11]:=
```
IntegerDigits[wiadomosc, 2, 5]
```

Out[11]=
```
{{1, 1, 0, 0, 0}, {1, 1, 0, 1, 0}, {1, 1, 0, 1, 1}, {0, 0, 1, 1, 0}, {0, 1, 1, 0, 0},
 {1, 1, 0, 1, 1}, {0, 1, 1, 0, 1}, {0, 1, 0, 0, 0}, {0, 0, 0, 0, 0}, {0, 0, 1, 0, 0},
 {1, 1, 1, 0, 1}, {0, 0, 0, 1, 1}, {0, 0, 1, 1, 1}, {1, 0, 1, 1, 1}, {0, 0, 0, 1, 1},
 {0, 0, 1, 1, 1}, {1, 1, 1, 1, 0}, {1, 0, 1, 1, 0}, {0, 1, 1, 0, 0}, {0, 0, 1, 1, 1},
 {0, 0, 1, 0, 0}, {1, 1, 1, 1, 0}, {0, 0, 1, 1, 1}, {1, 0, 0, 1, 1}, {1, 1, 0, 0, 0},
 {1, 1, 0, 1, 0}, {1, 1, 1, 0, 0}, {1, 0, 1, 0, 0}, {0, 0, 0, 0, 0}, {0, 0, 0, 1, 1},
 {1, 0, 1, 0, 0}, {0, 0, 0, 0, 0}, {0, 1, 1, 1, 1}, {1, 1, 0, 1, 1}, {0, 0, 0, 1, 1},
 {0, 1, 1, 0, 0}, {0, 1, 0, 0, 0}, {0, 0, 0, 0, 0}, {0, 1, 1, 1, 0}, {1, 0, 1, 1, 1},
 {1, 1, 1, 0, 1}, {1, 0, 1, 1, 0}, {1, 1, 0, 1, 0}, {1, 0, 1, 0, 0}, {0, 1, 0, 1, 0},
 {1, 0, 1, 1, 1}, {0, 0, 0, 0, 1}, {0, 1, 0, 0, 1}, {0, 1, 1, 0, 0}, {0, 1, 0, 0, 0}}
```

In[12]:=
```
zamianaKluczaNaCiagBinarny = IntegerDigits[kluczK, 2, 5]
```

Out[12]=
```
{{1, 0, 1, 0, 1}, {0, 1, 1, 1, 0}, {1, 1, 0, 0, 0}, {1, 0, 0, 1, 0}, {1, 0, 0, 0, 1},
 {0, 0, 1, 1, 1}, {1, 1, 0, 1, 0}, {0, 0, 1, 0, 0}, {1, 1, 0, 0, 1}, {1, 1, 1, 0, 1},
 {0, 0, 0, 1, 0}, {1, 1, 1, 0, 1}, {0, 1, 0, 1, 1}, {0, 0, 0, 0, 0}, {0, 0, 1, 1, 0},
 {0, 1, 1, 0, 0}, {0, 0, 0, 0, 1}, {1, 0, 0, 0, 0}, {0, 0, 0, 1, 1}, {0, 1, 0, 0, 0},
 {1, 1, 0, 1, 1}, {1, 0, 1, 1, 1}, {1, 1, 1, 0, 1}, {0, 0, 0, 1, 0}, {0, 1, 0, 0, 0},
 {1, 0, 1, 1, 0}, {0, 1, 1, 0, 1}, {1, 1, 1, 1, 0}, {1, 0, 0, 0, 1}, {0, 0, 0, 1, 1},
 {1, 1, 1, 0, 0}, {1, 1, 0, 1, 0}, {1, 1, 1, 0, 0}, {0, 0, 1, 1, 1}, {1, 0, 0, 1, 1},
 {0, 0, 1, 0, 1}, {0, 1, 0, 1, 1}, {1, 1, 1, 0, 0}, {0, 1, 0, 0, 1}, {1, 1, 1, 1, 1},
 {1, 1, 1, 1, 1}, {1, 0, 1, 1, 1}, {0, 0, 1, 0, 0}, {0, 1, 0, 0, 0}, {1, 1, 1, 0, 0},
 {1, 0, 1, 0, 0}, {0, 0, 1, 1, 1}, {0, 0, 0, 0, 1}, {0, 1, 0, 0, 1}, {0, 0, 1, 1, 1}}
```

In[13]:=
```
zaszyfrowanyTekst = BitXor[wiadomosc, kluczK]
```

Out[13]=
```
{13, 20, 3, 20, 29, 28, 23, 12, 25, 25, 31, 30, 12, 23, 5, 11, 31, 6, 15, 15, 31, 9, 26, 17,
 16, 12, 17, 10, 17, 0, 8, 26, 19, 28, 16, 9, 3, 28, 7, 8, 2, 1, 30, 28, 22, 3, 6, 8, 5, 15}
```

In[16]:=
```
IntegerDigits[zaszyfrowanyTekst, 2, 5] // Column
```

Out[16]=
```
{0, 1, 1, 0, 1}
{1, 0, 1, 0, 0}
{0, 0, 0, 1, 1}
{1, 0, 1, 0, 0}
{1, 1, 1, 0, 1}
{1, 1, 1, 0, 0}
{1, 0, 1, 1, 1}
{0, 1, 1, 0, 0}
{1, 1, 0, 0, 1}
{1, 1, 0, 0, 1}
{1, 1, 1, 1, 1}
{1, 1, 1, 1, 0}
{0, 1, 1, 0, 0}
{1, 0, 1, 1, 1}
{0, 0, 1, 0, 1}
{0, 1, 0, 1, 1}
{1, 1, 1, 1, 1}
{0, 0, 1, 1, 0}
{0, 1, 1, 1, 1}
{0, 1, 1, 1, 1}
{1, 1, 1, 1, 1}
{0, 1, 0, 0, 1}
{1, 1, 0, 1, 0}
{1, 0, 0, 0, 1}
{1, 0, 0, 0, 0}
{0, 1, 1, 0, 0}
{1, 0, 0, 0, 1}
{0, 1, 0, 1, 0}
{1, 0, 0, 0, 1}
{0, 0, 0, 0, 0}
{0, 1, 0, 0, 0}
{1, 1, 0, 1, 0}
{1, 0, 0, 1, 1}
{1, 1, 1, 0, 0}
{1, 0, 0, 0, 0}
{0, 1, 0, 0, 1}
{0, 0, 0, 1, 1}
{1, 1, 1, 0, 0}
{0, 0, 1, 1, 1}
{0, 1, 0, 0, 0}
{0, 0, 0, 1, 0}
{0, 0, 0, 0, 1}
{1, 1, 1, 1, 0}
{1, 1, 1, 0, 0}
{1, 0, 1, 1, 0}
{0, 0, 0, 1, 1}
{0, 0, 1, 1, 0}
{0, 1, 0, 0, 0}
{0, 0, 1, 0, 1}
{0, 1, 1, 1, 1}
```

zad.2

Nie można odczytać trzeciego bajtu tekstów jawnych wyłącznie na podstawie podanych szyfrogramów i zaszyfrowania ich tym samym kluczem, ponieważ brakuje dodatkowych informacji o samych tekstach jawnych. Te dane pozwalają nam jedynie na ustalenie różnic między tekstami, ale nie pozwalają ustalić ich wartości.