**Zestaw 4**

# Zadanie 1

Proszę zaszyfrować wiadomość *AGH UNIVERSITY*:

a) stosując szyfr Cezara $f(p) = (p + 2) \text{mod } 26$

b) stosując szyfr afiniczny $f(p) = (5p + 4) \text{mod } 26$

c) stosując szyfr transpozycyjny wykorzystujący permutację

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$$

d) stosując zamianę alfabetu z kluczem *WFIIS*

e) stosując szyfr Vigenere'a z kluczem: *WFIIS*

f) stosując szyfr Beauforta z kluczem: *WFIIS*

g) stosując szyfr Playfaira/Wheatstone'a z kluczem *WFIIS*

h) stosując szyfr XOR z kluczem *WFIIS*

# Zadanie 2

Używając szyfrowania RSA dla liczb klucza $(91, 5)$ proszę zaszyfrować wiadomość *AGH UNIVERSITY* (ASCII).

# Zadanie 3

Używając szyfrowania RSA dla $p = 43$, $q = 59$ oraz $e = 17$ zaszyfrować wiadomość $ATTACK$ (Lp.).

# Zadanie 4

Otrzymano wiadomość 3185 2038 2460 2550. Jak brzmi oryginalna wiadomość, jeżeli została zaszyfrowana ona szyfrem RSA z kluczem $(53 \cdot 61, 17)$

Tabela do zadań:

| Litera | Lp. | ASCII | Litera | Lp. | ASCII |
|---|---|---|---|---|---|
| **A** | 0 | 65 | **N** | 13 | 78 |
| **B** | 1 | 66 | **O** | 14 | 79 |
| **C** | 2 | 67 | **P** | 15 | 80 |
| **D** | 3 | 68 | **Q** | 16 | 81 |
| **E** | 4 | 69 | **R** | 17 | 82 |
| **F** | 5 | 70 | **S** | 18 | 83 |
| **G** | 6 | 71 | **T** | 19 | 84 |
| **H** | 7 | 72 | **U** | 20 | 85 |
| **I** | 8 | 73 | **V** | 21 | 86 |
| **J** | 9 | 74 | **W** | 22 | 87 |
| **K** | 10 | 75 | **X** | 23 | 88 |
| **L** | 11 | 76 | **Y** | 24 | 89 |
| **M** | 12 | 77 | **Z** | 25 | 90 |

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

Przykładowe wartości klucza RSA w praktyce:

- $n$ = 21513406576833588942900279145747846222398271830133160699503015317419057368114142720804148016150888717142822628552771258779244265031680385747899543144745380755520287547271377150427461263891601432377480572259560910463795299999833167903873276929738732983033512716764475188143371460456370582568565788402826226890109526038147408272900350308547442883919320868202708335058024775485093971791805607930562816222639149425652618190543679353432862421647514552818370821129983758341742258752547300322728678566227522454926542406996388081784798516634003112879834344747184190284577320899378194047931163370765960396891344513434816791563

- $e$ = 65537