SZYFR CEZARA AFINICZNY

- szyfrowanie $y = ax + b \pmod n$
  - a, b – liczby całkowite
  - $a \neq 0$
  - $b < n$
  - $NWD(a, n) = 1$
- deszyfrowanie $x = a^{-1}(y-b) \pmod n$ $\quad a^{-1}a = 1 \bmod n$
- <u>przykład</u>

$n = 26 \quad a = 3 \quad b = 5$

	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
x	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
$3x+5 \pmod{26}$	5	8	11	14	17	20	23	0	3	6	9	12	15	18	21	24	1	4	7	10	13	16	19	22	25	2
	F	I	L	O	R	U	X	A	D	G	J	M	P	S	V	Y	B	E	H	K	N	Q	T	W	Z	C

I) zaszyfrować 'KUL' $\quad K = 10 \quad U = 20 \quad L = 11$

$y = ax + b \pmod n$

$y = 3x + 5 \pmod{26}$

$x_1 = 10 \Rightarrow y_1 = 09$

$x_2 = 20 \Rightarrow y_2 = 13$

$x_3 = 11 \Rightarrow y_3 = 12$

Wiadomość zaszyfrowana: JNM

II) odszyfrować 'JNM'

$x = a^{-1}(y-b) \pmod n$

$26 = 3 \cdot 8 + 2$
$3 = 2 \cdot 1 + 1$
$2 = 1 \cdot 2 + 0$

$1 = 3 - 2 \cdot 1$
$1 = 3 - [26 - 3 \cdot 8]$
$1 = 3 - 26 - 3 \cdot 8$
$1 = 3 \cdot \underline{9} - 26$

} szukamy liczby odwrotnej do 'a' (a^{-1}) // jest to odwrotność modularna

$a^{-1} = 9$ // odwrotnością modularną jest liczba x z rozszerzonego algorytmu Euklidesa

$x = 9(y-5) \pmod{26}$

$x_1 = 9(9-5) \pmod{26} = 9 \cdot 4 \pmod{26} = 10 \Rightarrow K$

$x_2 = 9(13-5) \pmod{26} = 9 \cdot 8 \pmod{26} = 20 \Rightarrow U$

$x_3 = 9(12-5) \pmod{26} = 9 \cdot 7 \pmod{26} = 11 \Rightarrow L$

Wiadomość odszyfrowana: KUL