# Kodowanie i bezpieczeństwo informacji

## Lista nr 1 na 19 lutego-2 marca 2012

**Zadanie 1** Podaj formalne definicje funkcji $Gen, Enc, Dec$ dla schematów szyfrowania: Vigenere'a, Cezara (Shift), Substitution, Affine Cipher.

**Zadanie 2** Pokaż, że szyfry: Vigenera'a, Cezara (Shift) oraz podstawieniowy (Substitution) są podatne na:

- atak typu *known-plaintext*,
- atak typu *chosen-plaintext*.

Ile znaków tekstu jawnego potrzeba, aby całkowicie wydobyć klucz? Porównaj siłę ataków.

**Zadanie 3** (Powtórka z algebry)

- oblicz: $7503 \bmod 81$; $-7503 \bmod 81$; $81 \bmod 7503$; $-81 \bmod 7503$.
- wypisz wszystkie elementy odwracalne w $Z_m$ dla $m = 28, 33, 35$.
- znajdź liczbę elementów odwracalnych w $Z_m$ dla $m$ równego numerowi Twojego indeksu oraz dla $m$ będącego "iloczynem" Twojej daty urodzenia $m = rok * miesiac * dzie$ (np. $m = 1905 * 08 * 16$, kto się wtedy urodził?).

**Zadanie 4** (powtórka c.d.) Korzystając ze wzorów, a nie kalkulatora...

- znajdź $gcd(312, 403)$.
- znajdź takie $a, b$, że $312a + 403b = gcd(312, 403)$.
- wypisz elementy $Z_{21}^*$
- oblicz $2^{123} \bmod 35$.
- oblicz $2^{19} \bmod 19$.
- onajdź $93^{-1}$ w $Z_{1223}$.

**Zadanie 5** Znajdź i udowodnij złożoność algorytmu Euklidesa.

**Zadanie 6** Określ rozmiar przestrzeni kluczy szyfru afinicznego nad $Z_m$ dla $m = 30, 100, 1225$. Podaj wzór ogólny.