Historia i podstawy kryptografii
Spotkanie 2
Kilka użytecznych pojęć

Jacek Rogowski

I Liceum Ogólnokształcące
w Łowiczu

Podstawowe pojęcia

Elementy kryptosystemu

- *Algorytm szyfrowania* — niezmienny w obrębie danego kryptosystemu.
  Algorytm szyfrowania jest **na ogół** jawny.
- *Klucz* — dowolnie wymieniany, służący do zainicjowania konkretnej procedury przekształcenia tekstu jawnego w tekst tajny.
  Klucz jest **zawsze** tajny.

Kilka użytecznych pojęć — podejście nieformalne

- *Tekst jawny* to oryginalna wiadomość przed zaszyfrowaniem.
- *Tekst tajny (szyfrogram, kryptogram)* jest to wiadomość po zaszyfrowaniu.
- *Szyfrowaniem* nazywamy przekształcanie wiadomości jawnej w tekst zaszyfrowany.
- *Deszyfrowanie* to przekształcanie tekstu tajnego w jawny, również w przypadku, gdy klucz nie jest znany osobom dokonującym deszyfracji (mówi się wtedy o *łamaniu szyfru*).

Klasyfikacja szyfrów

Podstawowe typy szyfrów

- *Szyfry podstawieniowe* są szyframi, w których każda litera (lub ciąg liter) zostaje zastąpiony pewnym umownym znakiem, ale nie zmienia swojego miejsca w tekście.
- *Szyfry przestawieniowe* to szyfry, w których każda litera tekstu jawnego zmienia swoją pozycję w tekście, ale zachowuje swoją tożsamość; w wyniku stosowania takiego szyfru otrzymujemy *anagram* tekstu jawnego.
- *Szyfry mieszane*.

Klasyfikacja szyfrów podstawieniowych

- *Szyfry monoalfabetyczne*, w których każdemu znakowi alfabetu jawnego odpowiada zawsze ten sam znak alfabetu tajnego.
- *Szyfry polialfabetyczne*, w których używa się wielu alfabetów tajnych i każdy znak tekstu jawnego jest szyfrowany za pomocą jednego z tych alfabetów, wybranego w pewien ustalony sposób.

Klasyfikacja szyfrów

Klasyfikacja szyfrów ze względu na wielkość przekształcanych jednostek tekstu jawnego

- *Szyfry blokowe*
- *Szyfry strumieniowe*

Klasyfikacja szyfrów ze względu na postać klucza

- *Szyfry symetryczne*
- *Szyfry asymetryczne*