Zagadnienia do egzaminu z kryptografii

- Szyfr Vernama
- DES — schemat działania
- Tryby szyfrowania
- IDEA — schemat działania
- RSA — zasada działania
- Twierdzenie o rozkładzie na czynniki pierwsze
- Algorytm Euklidesa
- Rozszerzony algorytm Euklidesa
- Znajdowanie $a^{-1} \bmod m$
- Małe twierdzenie Fermata
- Chińskie twierdzenie o resztach
- Funkcja Eulera i twierdzenie Eulera
- Potęgowanie modulo metodą iterowanego podnoszenia do kwadratu
- Test Fermata pierwszości liczb
- Test Millera-Rabina
- Reszty kwadratowe w $\mathbb{Z}_p^*$
- Symbol Legendre'a i jego własności
- Reszty kwadratowe w $\mathbb{Z}_n^*$
- Symbol Jacobiego
- Logarytm dyskretny
- Algorytm ElGamala
- Jednokierunkowe funkcje hashujące i ich własności

- Synchroniczne szyfrowanie strumieniowe
- Asynchroniczne (samosynchronizujące) szyfrowanie strumieniowe
- Generatory ciągów pseudolosowych LFSR
- Generator Geffe
- Generator Blum-Micali
- Generator RSA
- Podpis cyfrowy ogólne własności
- Ślepe podpisy cyfrowe
- Uwierzytelnianie — protokół challenge-response
- Dowody z wiedzą zerową — ogólne własności
- Algorytm Diffiego-Hellmana
- Kryptoanaliza — rodzaje ataku
- Kryptoanaliza różnicowa — zasadnicza idea
- Kwantowe bramki logiczne
- Problem Deutscha
- Algorytm Shora
- Protokół BB84
- Protokół B92