

Algorytmy DES i IDEA na tle współczesnych algorytmów szyfrujących

Streszczenie.....1

1. Historia kryptografii.....3

1.1. Początki kryptografii.....3

1.2. Era komputerowa. Algorytmy symetryczne i asymetryczne.....4

1.3. Powstanie algorytmu DES.....4

1.4. Powstanie Algorytmu IDEA.....6

2. Mechanizmy stosowane we współczesnych algorytmach kryptograficznych.....6

2.1. Pojęcie klucza.....7

2.2. Kryptografia symetryczna.....11

2.3. Kryptografia z kluczem jawnym.....12

2.4. Arytmetyka modułarna.....13

2.5. Mieszanie i rozpraszanie.....14

2.6. Faktoryzacja. Generowanie liczb pierwszych.....15

3. Algorytmy DES i IDEA.....18

3.1. DES.....18

3.2. IDEA.....19

4. Inne algorytmy symetryczne.....21

4.1. Algorytm Rijndael.....21

4.2. Algorytm Blowfish.....	22
4.3. Algorytmy RC2 i RC4.....	22
4.4. Algorytm RC5.....	23
4.5. Algorytm Skipjack.....	23
4.6. SAFER.....	23

5. Algorytmy asymetryczne.....24

5.1. Algorytm Diffiego-Hellmana.....	24
5.2. Rozszerzony algorytm Diffiego-Hellmana.....	24
5.3. RSA.....	25
5.4. Algorytm ElGamala.....	26

6. Podsumowanie.....27

6.1. Zabezpieczenie dawane przez system kryptograficzny.....	27
6.2. Kryptoanaliza.....	28
6.3. Porównanie kryptografii z kluczem jawnym z kryptografią symetryczną.....	30

Literatura.....32