

Technologie podpisów cyfrowych – funkcjonowanie i zastosowania

Wprowadzenie.....4

Cel i zakres pracy.....6

Rozdział 1.

Wprowadzenie do kryptografii.....8

Rozdział 2.

Techniki kryptograficzne.....11

2.1. Protokoły arbitrazowe.....11

2.1.1. Protokoły rozjemcze.....13

2.1.2. Protokoły samowymuszające.....14

2.1.3. Protokoły

2.2. Zaawansowane algorytmy szyfrowania danych
DES.....14

2.2.1. Algorytm RSA.....24

2.2.2. Algorytm IDEA.....27

2.2.3. Międzynarodowy algorytm szyfrowania danych
MD5.....37

2.2.4. Algorytm SKIPJAC.....39

2.2.5. Algorytm

2.3. Inne algorytmy szyfrowania asymetrycznego Hellmana.....41

2.3.1. Algorytm Diffiego-ElGamala.....45

2.3.2. Algorytm szyfrowaniu.....46

2.3.3. Zastosowanie krzywych eliptycznych w

2.4. Techniki szyfrowania danych
strumieniowe.....49

2.4.1. Szyfry synchroniczne.....	50
2.4.2. Szyfry strumieniowe sie.....	51
2.4.3. Szyfry strumieniowe, samosynchronizujące blokowe.....	52
2.4.4. Szyfry szyfrowania.....	55
2.4.5. Nowoczesne metody jednorazowym.....	57
2.4.6. Algorytm oparty na kluczu	

Rozdział 3.

Podpis cyfrowy.....58

3.1. Podpis cyfrowy a odreczny.....	59
3.2. Tworzenie podpisu cyfrowego.....	61
3.3. Szyfrowanie z kluczem jawnym.....	63

Rozdział 4.

Skrót wiadomosci a podpis cyfrowy.....67

4.1. Funkcja haszująca.....	67
4.2. Skrót wiadomosci.....	70
4.3. Algorytmy generowania skrótów.....	71
4.4. Podpisy cyfrowe.....	73

Rozdział 5.

Ochrona danych w sieci i intersieci.....81

Rozdział 6.

Ramy prawne dla podpisu cyfrowego.....84

6.1. Ustawy modelowe UNCITRAL.....	84
6.2. Dyrektywa Parlamentu Europejskiego i Rady Unii Europejskiej.....	84
6.3. Polska ustawa.....	86
6.4. Znacznik czasu.....	90
6.5. Certyfikaty.....	90

Podsumowanie..... 96

Literatura..... 98