

Algorytmy DES i IDEA – opis i prezentacja

Wstęp3

Cel i zakres pracy4

Rozdział 1.

Pojęcie operacji szyfrowania i konieczność jej realizacji

1.1. Cele ochrony informacji 6

Rozdział 2.

Model systemu szyfrowania i jego elementy

2.1. Pojęcie protokołu kryptograficznego..... 9

2.2. Pojęcie klucza..... 9

2.3. Funkcje jednokierunkowe i funkcje skrótu – integralność danych 9

2.4. Podpisy cyfrowe..... .12

2.5. Usługi znakowania czasowego..... 13

2.6. Kryptografia symetryczna 14

2.7. Kryptografia z kluczem jawnym 15

Rozdział 3.

Wybrane podstawowe algorytmy szyfrujące – przegląd

3.1. Szyfry podstawieniowe i przestawieniowe..... 17

3.2. Era komputerowa. algorytmy symetryczne i asymetryczne.....
19

3.3. Przykłady obecnie stosowanych algorytmów 20

Rozdział 4.

Pojęcie kluczy szyfrowania i ich klasyfikacja

4.1. Generowanie kluczy 25

4.2. Przesyłanie kluczy.....	26
4.3. Sprawdzanie kluczy	26
4.4. Stosowanie kluczy	27
4.5. Przechowywanie kluczy.....	27
4.6. Klucze skompromitowane	27
4.7. Okres ważności kluczy.....	28
4.8. Certyfikaty kluczy jawnych	28
4.9. Rozproszone zarządzanie kluczami.....	29

Rozdział 5.

Moc szyfrowania.....30

Rozdział 6.

Kryptoanaliza32

Rozdział 7.

Przykłady wykorzystania technik kryptograficznych

7.1. Szyfrowanie danych do przechowywania	35
7.2. Cyfrowe pieniądze.....	37
7.3. Poczta elektroniczna.....	40
7.4. Kryptografia w internecie	43

Rozdział 8.

Algorytm des

8.1. Historia standardu.....	46
8.2. Opis działania	47
8.3. Przekształcenia klucza	52
8.4. Tryby pracy algorytmu des.....	54

Rozdział 9.

Algorytm idea

9.1. Podstawowe wiadomości	58
----------------------------------	----

9.2. Opis działania	59
9.3. Przekształcenia klucza	62
9.4. Bezpieczeństwo i implementacje.....	63

Rozdział 10.

Ataki na algorytmy des i idea.

10.1. Atak wyczerpujący	65
10.2. Analiza kryptograficzna.....	66
10.3. Ataki na system szyfrujący.....	67

Podsumowanie

Literatura