

Ewolucja metod szyfrowania danych w systemie informatycznym

>

Cel i zakres pracy.....5

18:37 2009-11-23

1. Wprowadzenie – potrzeba szyfrowanych danych..... 6

2. Teoria złożoności obliczeniowej..... 8

3.
przegląd podstawowych algorytmów szyfrowania..... 9

3.1. Szyfry przestawieniowe.....9

3.2. Szyfry podstawieniowe9

3.3. Szyfry kaskadowe12

4. Szyfrowanie wielokropkowe..... 13

4.1. Szyfrowanie dwukrotne13

4.2. Szyfrowanie trzykrotne.....13

5. Szyfry blokowe i strumieniowe..... 15

5.1. Szyfry strumieniowe15

5.1.1. Samosynchronizujące szyfry strumieniowe17

5.1.2. Generatory ciągów.....17

5.2. Szyfry blokowe.....20

5.2.1. DES – Data Encryption Standard20

5.2.1.1 Permutacja początkowa i końcowa.....21

5.2.1.2 Kodowanie.....	22
5.2.1.3 Deszyfrowanie	24
5.2.2. Warianty działania algorytmu DES.....	24
5.2.2.1 Elektroniczna ksiazka kodowa – Electronical Codebook	25
5.2.2.2 Tryb wiazania bloków – Cipher Block Chaning	26
5.2.2.3 Sprzezenie zwrotne – Cipher Feedback	27
5.2.3. Modyfikacje algorytmu DES.....	27
5.2.4. IDEA – International Data Encryption Standard.....	28
5.2.5. Algorytm Madrygi	29
5.2.6. Algorytm RC 5	30

6. Algorytmy z kluczem jawnym.....32

6.1. Algorytm Diffiego – Hellmana	32
6.2. Szyfry plecakowe	33
6.2.1. Plecaki (ciagi) superrosnace	34
6.2.2. Utajnianie ciagu superrosnacego	34
6.2.3. Kodowanie i dekodowanie wiadomosci za pomoca otrzymanego klucza.....	35
6.3. RSA	35
6.3.1. Trudnosci wynikajace podczas wykonywania algorytmu	36
6.3.2. Tworzenie bezpiecznych kluczy.....	36
6.3.3. Kryptoanaliza algorytmu RSA	37
6.4. Algorytm podpisywania Fiata-Shamira	38
6.5. Algorytm Feiego-Fiata-Shamira	38
6.5.1. Algorytm identyfikacyjny Feiego-Fiata-Shamira	39
6.6. Zasady chronienia kluczy	39
6.7. Tworzenie kluczy	41

7. Nowoczesne algorytmy szyfrowania..... 44

7.1. Ogólne zalozenia algorytmu AES.....	44
7.1.1. Bajty.....	44

7.1.2. Tablice bitów	45
7.1.3. Tablica Stanów	45
7.1.4. Specyfikacja algorytmu	46
7.1.4.1 Szyfrowanie	47
7.1.4.1.1 Zastępowanie bajtów z wykorzystaniem S – bloków.....	47
7.1.4.1.2 Zamienianie rzędów tablicy Stanu przez offsety.....	48
7.1.4.1.3 Przemieszczanie danych z kolumnami tablicy.....	49
7.1.4.1.4 Dodanie Klucza Cyklu do tablicy.....	50
7.1.4.1.5 Klucz Ekspansji	50
7.1.4.2 Deszyfrowanie	51
7.1.4.2.1 InvShiftRows()	51
7.1.4.2.2 InvSubBytes().....	52
7.1.4.2.3 InvMixColumns()	52
7.1.4.2.4 AddRoundKey()	53
7.2. Algorytm SKIPJACK	54
7.2.1. Etapy szyfrowania	55
7.2.2. Permutacja G	55

8. Kryptoanaliza..... 57

8.1. Czynniki oddziałujące na bezpieczeństwo kryptografii.....	57
8.2. Klasy łamania szyfrogramów	58
8.3. Kroki kryptoanalizy	59
8.4. Podstawowe wiadomości potrzebne do kryptoanalizy	60
8.4.1. Charakterystyka języka.....	60
8.4.2. Jednostronny rozkład częstotliwości	61
8.4.3. Wskaznik zgodności	61
8.4.4. Test Phi	62

9. Odzyskiwanie szyfrów przestawieniowych..... 64

9.1. Określanie rozmiaru macierzy	64
9.2. Odzyskiwanie zawartości macierzy przy pomocy anagramów	64

10. Lamanie szyfrow podstawieniowych..... 67

10.1. Odzyskiwanie szyfrów monoalfabetycznych67

10.1.1. Odzyskiwanie alfabetu z jednym ciągiem znakowym67

10.1.2. Odzyskiwanie alfabetu z dwoma przemieszczanymi ciągami znakowymi68

10.1.3. Szyfry monoalfabetyczne używające jako szyfru mieszanych alfabetów69

10.1.3.1 Test chi69

10.1.3.2 Odzyskiwanie szyfrogramów za pomocą prawdopodobieństwa występowania słów.....70

10.2. Ataki na systemy poligramowe76

10.2.1. Test zgodności dla digramów – Phi Test.....76

10.2.2. Atak na szyfr poligramowy Playfaira.....77

10.3. Ataki na szyfry wieloalfabetowe82

10.3.1. Metoda prawdopodobieństwa występowania wyrazów.....82

Podsumowanie 86

Literatura..... 87