

Łamanie zabezpieczeń kryptograficznych

Streszczenie..... 2

Rozdział 1.

Kryptoanaliza

1.1. Klasy łamania szyfrogramów..... 4

1.2. Podstawowe wiadomości potrzebne do kryptoanalizy..... 5

1.2.1. Charakterystyka języka..... 5

1.2.2. Jednostronny rozkład częstotliwości 6

1.2.3. Wskaźnik zgodności 6

1.2.4. Test Phi 7

Rozdział 2.

Nowoczesne algorytmy szyfrowania

2.1. Ogólne założenia algorytmu AES 8

2.1.1. Bajty.....8

2.1.2. Tablice bitów9

2.1.3. Tablica Stanów9

2.1.4. Specyfikacja algorytmu 10

2.1.4.1 Szyfrowanie 10

2.1.4.1.1 Zastępowanie bajtów z wykorzystaniem S – bloków..... 11

2.1.4.1.2 Zamienianie rzędów tablicy Stanu przez offsety..... 11

2.1.4.1.3 Przemieszczanie danych z kolumnami tablicy..... 12

2.1.4.1.4 Dodanie Klucza Cyklu do tablicy..... 12

2.1.4.1.5 Klucz Ekspansji 12

2.1.4.2 Deszyfrowanie 13

Rozdział 3.

Łamanie szyfrów przestawieniowych

3.1. Określanie rozmiaru macierzy..... 13

3.2. Odzyskiwanie zawartości macierzy przy pomocy anagramów.....

Rozdział 4.**Łamanie szyfrów podstawieniowych**

- 4.1. Odzyskiwanie szyfrów monoalfabetycznych 15
 - 4.1.1. Odzyskiwanie alfabetu z jednym ciągiem znakowym 16
 - 4.1.2. Odzyskiwanie za pomocą prawdopodobieństwa występowania słów 17
- 4.2. Ataki na systemy poligramowe 22
 - 4.2.1. Atak na szyfr poligramowy Playfaira..... 22
- 4.3. Ataki na szyfry wieloalfabetowe 27
 - 4.3.1. Metoda prawdopodobieństwa występowania wyrazów 28

Literatura 30