

Część I. Kryptografia (13)

1.. Streszczenie wstępne (23)

- 1.1. Kryptografia i steganografia (23)
- 1.2. Semagramy (24)
- 1.3. Kod jawny: maskowanie (28)
- 1.4. Wskazówki (31)
- 1.5. Kod jawny: woalowanie za pomocą wartości zerowych (33)
- 1.6. Kod jawny: woalowanie za pomocą kratki (38)
- 1.7. Klasyfikacja metod kryptograficznych (39)

2. Cele i metody kryptografii (41)

- 2.1. Natura kryptografii (41)
- 2.2. Szyfrowanie (47)
- 2.3. Systemy kryptograficzne (kryptosystemy) (49)
- 2.4. Polifonia (52)
- 2.5. Zbiory znaków (54)
- 2.6. Klucze (56)

3. Kroki szyfrowania: podstawienie proste (59)

- 3.1. Przypadek $V^{(1)} \rightarrow W$ (jednodzielne podstawienia proste) (59)
- 3.2. Przypadek szczególny $V \leftrightarrow V$ (permutacje) (61)
- 3.3. Przypadek $V^{(1)} \rightarrow W^m$ (wielodzielne podstawienia proste) (68)
- 3.4. Przypadek ogólny $V^{(1)} \rightarrow W^{(m)}$ (rozstawianie) (71)

4. Kroki szyfrowania: podstawienie i kodowanie poligraficzne (75)

- 4.1. Przypadek $V^2 \rightarrow W^{(m)}$ (podstawienie dwuznakowe) (75)
- 4.2. Przypadek szczególny Playfaira i Delastelle'a: metody tomograficzne (81)
- 4.3. Przypadek $V^3 \rightarrow W^{(m)}$ (podstawienie trójznakowe) (85)
- 4.4. Przypadek ogólny $V^{(n)} \rightarrow W^{(m)}$: kody (85)

5. Kroki szyfrowania: podstawienie liniowe 99

- 5.1. Samoodwrotne podstawienia liniowe (101)
- 5.2. Jednorodne podstawienia liniowe (102)
- 5.3. Binarne podstawienia liniowe (106)
- 5.4. Ogólne podstawienia liniowe (106)
- 5.5. Rozłożone podstawienia liniowe (107)
- 5.6. Alfabet dziesiętkowane (110)
- 5.7. Podstawienia liniowe dla liczb dziesiętnych i binarnych (110)

6. Kroki szyfrowania: transpozycja (113)

- 6.1. Najprostsze metody (113)
- 6.2. Transpozycja kolumnowa (117)
- 6.3. Anagramy (121)

7. Szyfrowanie polialfabetyczne: rodziny alfabetów (125)

- 7.1. Podstawienia iterowane (125)
- 7.2. Alfabetów przesunięte i obrócone (126)
- 7.3. Rotorowe maszyny szyfrujące (130)
- 7.4. Przesunięte alfabetów standardowe: Vigenčre i Beaufort (138)
- 7.5. Alfabetów niezależne (141)

8. Szyfrowanie polialfabetyczne: klucze (151)

- 8.1. Wczesne metody z kluczami okresowymi (151)
- 8.2. Klucz podwójny (153)
- 8.3. Szyfrowanie Vernama (154)
- 8.4. Klucze pseudonieokresowe (156)
- 8.5. Maszyny generujące własny ciąg znaków klucza (158)
- 8.6. Zewnętrzne tworzenie ciągów znaków klucza (168)
- 8.7. Klucze nieokresowe (170)
- 8.8. Klucze jednorazowe (173)
- 8.9. Negocjowanie kluczy i zarządzanie kluczami (176)

9. Składanie klas metod (181)

- 9.1. Grupy (181)
- 9.2. Przeszyfrowywanie (184)
- 9.3. Podobieństwo metod szyfrowania (186)
- 9.4. „Przekształcenie piekarza” Shannona (186)
- 9.5. Mieszanie i rozpraszanie za pomocą operacji arytmetycznych (192)
- 9.6. DES i IDEA (196)

10. Systemy z jawnym kluczem szyfrującym (205)

- 10.1. Symetryczne i asymetryczne metody szyfrowania (206)
- 10.2. Funkcje jednokierunkowe (208)
- 10.3. Metoda RSA (215)
- 10.4. Kryptoanalityczny atak na RSA (217)
- 10.5. Poufność a uwierzytelnianie (221)
- 10.6. Bezpieczeństwo systemów z kluczem publicznym (222)

11. Bezpieczeństwo szyfrowania (225)

- 11.1. Błędy kryptograficzne (225)
- 11.2. Zasady kryptologii (233)
- 11.3. Kryteria Shannona (238)
- 11.4. Kryptologia a prawa człowieka (239)

Część II. Kryptoanaliza (245)

12. Złożoność kombinatoryczna przeszukiwania wyczerpującego (251)

- 12.1. Monoalfabetyczne podstawienie proste (252)
- 12.2. Monoalfabetyczne szyfrowanie poligraficzne (253)

- 12.3. Szyfrowania polialfabetyczne (255)
- 12.4. Ogólne uwagi na temat złożoności kombinatorycznej (257)
- 12.5. Kryptoanaliza przez atak wyczerpujący (258)
- 12.6. Długość krytyczna (259)
- 12.7. Praktyczne stosowanie ataku wyczerpującego (262)
- 12.8. Mechanizacja ataku wyczerpującego (265)

13. Anatomia języka: wzorce (267)

- 13.2. Wykluczanie metod szyfrowania (270)
- 13.3. Wyszukiwanie wzorca (270)
- 13.4. Wyszukiwanie wzorców poligraficznych (274)
- 13.5. Metoda słów prawdopodobnych (274)
- 13.6. Automatyczne wyczerpywanie realizacji wzorca (279)
- 13.7. Pangramy (281)

14. Przypadek polialfabetyczny: słowa prawdopodobne (283)

- 14.1. Wyczerpywanie pozycji negatywnego wzorca słowa prawdopodobnego (283)
- 14.2. Wyczerpywanie pozycji binarnego negatywnego wzorca słowa prawdopodobnego (286)
- 14.3. Atak de Viarisa (288)
- 14.4. Wyczerpywanie pozycji słowa prawdopodobnego metodą zygzakową (295)
- 14.5. Metoda izomorfów (297)
- 14.6. Ukryta kompromitacja tekst jawny–kryptogram (302)

15. Anatomia języka: częstoci (305)

- 15.1. Wykluczanie metod szyfrowania (305)
- 15.2. Niezmienniczość partycji (307)
- 15.3. Metoda intuicyjna: profil częstoci (308)
- 15.4. Szeregowanie częstoci 310
- 15.5. Kliki i dopasowanie partycji (313)
- 15.6. Dopasowanie optymalne (318)
- 15.7. Częstoci wieloznaków (320)
- 15.8. Mieszana metoda dopasowania częstoci (328)
- 15.9. Dopasowanie wzorca w przypadku podstawień poligraficznych (332)
- 15.10. Styl dowolny (334)
- 15.11. Dodatkowe informacje o długości krytycznej (337)

16. Kappa i Chi (339)

- 16.1. Definicja i niezmienniczość parametru Kappa (339)
- 16.2. Definicja i niezmienniczość parametru Chi (342)
- 16.3. Twierdzenie Kappa–Chi (345)
- 16.4. Twierdzenie Kappa–Phi (346)
- 16.5. Symetryczne funkcje częstoci znaków (348)

17. Badanie okresowoci (351)

- 17.1. Test Kappa Friedmana (352)

- 17.2. Test Kappa dla wieloznaków (353)
- 17.3. Kryptoanaliza maszynowa (354)
- 17.4. Metoda Kasiskiego (360)
- 17.5. Nawarstwianie i test Phi Kullbacka (365)
- 17.6. Szacowanie długości okresu (368)

18. Ustawianie alfabetów towarzyszących (371)

- 18.1. Dopasowanie profilu (371)
- 18.2. Ustawianie względem znanego alfabetu (375)
- 18.3. Test Chi: wzajemne ustawianie alfabetów towarzyszących (379)
- 18.4. Rekonstrukcja alfabetu podstawowego (383)
- 18.5. Symetria pozycji Kerckhoffs (386)
- 18.6. Usuwanie przeszyfrowania: metoda różnicowa (391)
- 18.7. Deszyfrowanie kodu (393)
- 18.8. Rekonstrukcja hasła (394)

19. Kompromitacje (397)

- 19.1. Nakładanie Kerckhoffs (397)
- 19.2. Nakładanie metod szyfrowania posiadających grupę kluczy (399)
- 19.3. Zgodne fazowo nakładanie kodu przeszyfrowanego (415)
- 19.4. Kompromitacje kryptogram–kryptogram (418)
- 19.5. Metoda Sinkova (422)
- 19.6. Kompromitacja kryptogram–kryptogram: dublowanie wskaźnika (429)
- 19.7. Kompromitacja tekst jawny–kryptogram: cykl sprzężenia zwrotnego (444)

20. Kryptoanaliza liniowa (455)

- 20.1. Redukcja liniowych podstawień poligraficznych (455)
- 20.2. Rekonstrukcja klucza 456
- 20.3. Rekonstrukcja liniowego rejestru przesuwanego (457)

21. Anagramowanie (461)

- 21.1. Transpozycja (461)
- 21.2. Podwójna transpozycja kolumnowa (464)
- 21.3. Anagramowanie wielokrotne (465)

22. Uwagi końcowe (469)

- 22.1. Sukces w złamaniu szyfru (470)
- 22.2. Sposób działania niepowołanego deszyfranta (475)
- 22.3. Ułuda bezpieczeństwa (480)
- 22.4. Znaczenie kryptologii (481)

Aksjomatyczna teoria informacji (487)

- A.1. Aksjomaty aksjomatycznej teorii informacji (487)
- A.2. Aksjomatyczna teoria informacji kryptosystemów (489)

- A.3. Kryptosystemy zupełne i z kluczem niezależnym (491)
- A.4. Główne twierdzenie Shannona (493)
- A.5. Długość krytyczna (494)
- A.6. Kompresja kodowa (496)
- A.7. Niemożność totalnego nieuporządkowania (496)

Bibliografia (499)

Skorowidz (503)

Źródła fotografii (535)