

Kryptografia symetryczna, asymetryczna, a kryptografia kontrolowana

Rozdział 1

Poufnosc.....5

Rozdział 2

Algorytmy i standardy szyfrowania.....7

2.1 Algorytmy oparte o klucz symetryczny8

2.1.1 Algorytm DES..... 9

2.1.2 Potrójny DES9

2.1.3 Algorytm DESX..... 10

2.1.4 Algorytm IDEA10

2.1.5 Algorytm RC210

2.1.6 Algorytm RC411

2.1.7 Wybór algorytmu11

2.2 Kryptografia z kluczem jawnym11

2.3 Algorytmy klucza jawnego12

2.3.1 System kryptograficzny Rivesta-Schamira-Adlemana12

2.3.2 Algorytm ElGamala.....12

2.3.3 Inne algorytmy z kluczem jawnym13

2.4 Wybieranie algorytmu z kluczem jawnym13

Rozdział 3

3.1 Uwierzytelnianie14

3.2 Podpisy cyfrowe..... 15

3.3 Algorytmy podpisów cyfrowych16

3.3.1 RSA.....16

3.3.2 DSA.....16

3.4 Podpisy cyfrowe i szyfrowanie.....17

Rozdział 4

4.1 Hierarchiczne poswiadczenie certyfikatów.....18

4.2 Rozproszone poswiadczenie certyfikatów.....18

4.3 Rozpowszechnianie certyfikatów19

Rozdział 5

5.1 Sposoby doboru hasła20

5.2 Kompresja danych21

5.3 Wymazywanie plików22

5.4 Konie trojanskie..... 23

5.5 Anonimowe odsyłanie poczty24

Rozdział 6

6.1 Patenty25

Rozdział 7

7.1 Ataki na algorytmy oparte o klucz symetryczny28

7.2 Ataki silowe29

7.3 Analiza kryptograficzna30

7.4 Ataki na algorytm szyfrujący30

7.4.1 Atak znanym tekstem jawnym30

7.4.2 Atak wybranym tekstem jawnym31

7.4.3 Kryptoanaliza różnicowa31

7.4.4 Różnicowa analiza błędów31

7.5 Ataki na system szyfrujący..... 32

7.6 Ataki na algorytmy bazujące na kluczu publicznym32

7.6.1 Ataki wykorzystujące rozkład na czynniki pierwsze33

7.6.2 Ataki algorytmiczne33

7.6.3 Skrótory wiadomości34

7.7 Ataki na generatory skrótory wiadomości..... 34

7.8 Zagrożenia związane z kryptografią35

Rozdział 8

8.1 Trzecia zaufana strona37

8.2 Zaufanie a odpowiedzialnosc..... 38

8.3 Zagrozenia38

Podsumowanie..... 40

Literatura.