

## Spis treści

Wstęp.....	7
<b>Ćwiczenie 1</b>	
<b>Temat: Bezpieczeństwo transmisji danych .....</b>	<b>9</b>
1.1. Cel ćwiczenia .....	9
1.2. Pytania kontrolne.....	9
1.3. Część praktyczna.....	9
1.3.1. Bezpieczeństwo protokołu Telnet .....	10
1.3.2. Bezpieczeństwo protokołu SSH .....	11
1.3.3. Bezpieczeństwo wirtualnych sieci prywatnych.....	13
1.3.4. Bezpieczeństwo użytkownika komunikatorów sieciowych.....	14
1.3.5. Atak <i>man in the middle</i> .....	14
1.3.6. Atak DoS (ang. <i>Denial of Service</i> ).....	16
1.3.7. Sprawozdanie .....	17
1.4. Literatura .....	17
<b>Ćwiczenie 2</b>	
<b>Temat: Szyfrowanie za pomocą algorytmów symetrycznych.....</b>	<b>19</b>
2.1. Cel ćwiczenia .....	19
2.2. Pytania kontrolne.....	19
2.3. Wprowadzenie.....	19
2.3.1. Informacje ogólne o kryptosystemie DES (ang. <i>Data Encryption Standard</i> ) .....	19
2.3.2. Informacje o RC2 i RC4.....	21
2.3.3. IDEA (ang. <i>International Data Encryption Algorithm</i> ) .....	22
2.3.4. AES (ang. <i>Advanced Encryption Standard</i> ).....	23
2.4. Zadania do wykonania.....	23
2.4.1. Własności DES.....	23
2.4.2. Porównanie kryptosystemów symetrycznych .....	25
2.5. Literatura .....	26
<b>Ćwiczenie 3</b>	
<b>Temat: Własności szyfru asymetrycznego – RSA .....</b>	<b>27</b>
3.1. Cel ćwiczenia .....	27
3.2. Pytania kontrolne.....	27
3.3. Wprowadzenie.....	27

3.3.1. Istota szyfru RSA .....	27
3.3.2. Generacja kluczy .....	28
3.3.3. Praktyczne zastosowanie szyfrów z kluczem publicznym .....	29
3.4. Realizacja ćwiczenia .....	29
3.5. Opracowanie wyników .....	31
3.6. Literatura .....	31

#### Ćwiczenie 4

##### **Temat: Własności funkcji skrótu i podpisu cyfrowego z zastosowaniem RSA.....**

4.1. Cel ćwiczenia .....	33
4.2. Pytania kontrolne.....	33
4.3. Wprowadzenie.....	33
4.3.1. Pożądane własności funkcji skrótu.....	33
4.3.2. Wykorzystanie funkcji skrótu do realizacji podpisu cyfrowego .....	34
4.4. Wykonanie ćwiczenia.....	35
4.4.1. Badanie własności funkcji skrótu .....	35
4.4.2. Realizacja podpisu cyfrowego.....	36
4.5. Literatura .....	38

#### Ćwiczenie 5

##### **Temat: Badanie podpisów cyfrowych generowanych przy użyciu różnych algorytmów .....**

5.1. Cel ćwiczenia laboratoryjnego .....	39
5.2. Pytania kontrolne.....	39
5.3. Wprowadzenie teoretyczne .....	39
5.3.1. Generowanie i weryfikacja podpisu cyfrowego .....	39
5.3.2. Podstawowe informacje o wybranych algorytmach wykorzystywanych w podpisie cyfrowym.....	41
5.3.3. Opis programów użytych w ćwiczeniu .....	48
5.4. Realizacja ćwiczenia .....	50
5.4.1. Badanie szybkości implementacji wybranych algorytmów .....	50
5.4.2. Podpisywanie wiadomości ECDSA .....	53
5.4.3. Podpisywanie wiadomości DSA .....	53
5.4.4. Podpisywanie wiadomości RSA.....	54
5.5. Sprawozdanie .....	55
5.6. Literatura .....	56

## Ćwiczenie 6

<b>Temat: Generacja i dystrybucja kluczy tajnych .....</b>	<b>57</b>
6.1. Cel ćwiczenia .....	57
6.2. Pytania kontrolne.....	57
6.3. Wprowadzenie.....	57
6.3.1. Podstawowa wersja algorytmu Diffiego–Hellmana .....	57
Atak od środka.....	58
Algorytm Diffiego–Hellmana z uwierzytelnieniem wiadomości.....	58
6.3.2. Algorytm ElGamala.....	59
6.3.3. Generacja kluczy w algorytmie DSA .....	60
Generowanie kluczy w algorytmie RSA .....	61
6.4. Realizacja ćwiczenia .....	61
6.4.1. Analiza algorytmu Diffiego–Hellmana .....	61
6.4.2. Generowanie i analiza kluczy w programie GnuPG .....	62
6.4.3. Eksportowanie i importowanie kluczy .....	65
Uzgadnianie kluczy z uwierzytelnieniem.....	66
6.5. Literatura .....	67

## Ćwiczenie 7

<b>Temat: Wybrane metody kryptoanalizy .....</b>	<b>69</b>
7.1. Cel ćwiczenia .....	69
7.2. Pytania kontrolne.....	69
7.3. Wprowadzenie teoretyczne .....	69
7.3.1. Szyfr Cezara .....	69
7.3.2. Szyfry symetryczne .....	70
7.3.3. Algorytm RC4 .....	71
7.3.4. Funkcje skrótu .....	71
7.3.5. Protokół SSL .....	72
7.3.6. Tęczowe tablice.....	73
7.4. Przebieg ćwiczenia .....	75
7.4.1. Szyfry historyczne przy wykorzystaniu programu CrypTool .....	75
7.4.2. Szyfry symetryczne przy wykorzystaniu programu CrypTool.....	76
7.4.3. Atak na funkcję skrótu.....	77
7.5. Literatura .....	78

## Ćwiczenie 8

<b>Temat: Realizacja szyfrowania z uwierzytelnieniem .....</b>	<b>79</b>
8.1. Cel ćwiczenia .....	79
8.2. Pytania kontrolne.....	79
8.3. Wprowadzenie teoretyczne .....	79
8.4. Realizacja ćwiczenia. ....	81
8.4.1. Szyfrowanie i deszyfrowanie pliku w trybie CTR (ang. <i>counter</i> ).....	81
8.4.2. Szyfrowanie i deszyfrowanie pliku w trybie INK .....	83
8.5. Zawartość sprawozdania .....	85
8.6. Literatura .....	86
<b>Zakończenie .....</b>	<b>87</b>