

SPIS TREŚCI

1. Wprowadzenie	11
2. Rozwój metod przesyłania i ochrony informacji	13
3. Szybkość przesyłu informacji cyfrowej	17
3.1. Media transmisyjne w sieciach komputerowych	18
4. Sieci bezprzewodowe i bezpieczeństwo przesyłanej informacji	27
4.1. Struktura cyfrowego systemu radiokomunikacyjnego	30
4.2. Dobór parametrów systemu radiokomunikacyjnego	31
4.2.1. Częstotliwości w systemach radiowych	31
4.2.2. Dobór mocy nadajnika	32
4.2.3. Systemy radiowe z widmem rozproszonym	32
4.3. Synchronizacja	33
4.4. Propagacja sygnałów radiowych wielkiej częstotliwości	34
4.5. Fale podczerwone	34
4.6. Światło laserowe (monochromatyczne)	36
4.7. Porównanie mediów bezprzewodowych	36
5. Urządzenia transmisji bezprzewodowej	37
5.1. Urządzenia wykorzystujące fale radiowe	37
5.2. Urządzenia wykorzystujące fale z zakresu podczerwieni	38
6. Realizacja komunikacji bezprzewodowej w sieciach komputerowych	39
6.1. Radiomodemy	41
6.2. Radiowe kontrolery pakietowe	41
6.3. Karty bezprzewodowych sieci lokalnych oraz punkty dostępu	41
6.4. Mosty bezprzewodowe	41
7. Istniejące systemy transmisji bezprzewodowej	43
7.1. Podział systemów transmisji bezprzewodowej	43
7.1.1. System komórkowy GSM	43
7.1.2. System DECT	44
7.1.3. Mobilne sieci rozległe	45
7.1.4. Sieci rozległe stacjonarne	45
7.2. Sieć Aloha	45
7.3. Bezprzewodowe sieci lokalne	46
8. Problemy techniczne w transmisji radiowej	47
8.1. Transmisja dwukierunkowa	47
8.2. Dostęp do łącza	47
8.3. Wybór trasy	48
9. Picosieci i sieci lokalne	51
9.1. Sieci typu picosieci oparte o standard Bluetooth	51
9.1.1. Ogólny opis sieci	51
9.1.2. Warstwa fizyczna	52

9.1.3.	Łącze danych	53
9.1.4.	Kanał transmisji	53
9.1.5.	Adresowanie	54
9.1.5.1.	Adres fizyczny	54
9.1.5.2.	Kod dostępu	54
9.1.6.	Adres urządzenia aktywnego	54
9.1.7.	Pakiety	54
9.1.8.	Korekcja błędów	55
9.1.9.	Bezpieczeństwo	56
9.1.9.1.	Autentyfikacja	56
9.2.	Sieci lokalne oparte o standard 802.11	56
9.2.1.	Elementy architektury i konfiguracje sieci zgodne ze standardem 802.11	57
9.2.2.	Metoda dostępu do łącza	60
9.2.3.	Format ramki	62
9.2.4.	Zasięg i odporność na zakłócenia urządzeń zgodnych ze standardem 802.11	62
9.2.5.	Bezpieczeństwo i autentyfikacja	63
10.	Sieci oparte o protokoły WAP	65
10.1.	Model WAP a model Internetu	66
10.2.	Architektura WAP	67
10.3.	Bezprzewodowe środowisko aplikacyjne (WAE)	68
10.4.	Protokoły WAP	68
10.5.	Ograniczone możliwości sieci	70
10.6.	Opis bibliotek standardowych WMLScript	71
11.	Podstawowe pojęcia kryptografii	75
11.1.	Kryptografia symetryczna	77
11.2.	Funkcje skrótu	77
11.3.	Kryptografia z kluczem jawnym	78
12.	Klasyczne algorytmy kryptograficzne	79
12.1.	Steganografia	79
12.2.	Szyfry podstawieniowe	79
12.3.	Szyfry przestawieniowe	80
12.4.	Szyfr jednokrotny	81
12.5.	System kryptograficzny	82
12.6.	Symetryczne algorytmy kryptograficzne	83
12.6.1.	Algorytm IDEA	83
12.6.1.1.	Operacje pojedynczego cyklu	84
12.6.1.2.	Operacje na podkluczach	84
12.6.1.3.	Deszyfrowanie IDEA	85
12.6.2.	Algorytm DES	85
12.6.2.1.	Permutacja początkowa	86
12.6.2.2.	Przekształcenia klucza	86

12.6.2.3. Podział tekstu na bloki	87
12.6.2.4. Permutacja rozszerzająca	87
12.6.2.5. Szyfrowanie przy użyciu S-bloków	87
12.6.2.6. Permutacje w P-blokach	87
12.6.2.7. Permutacja końcowa	88
12.6.2.8. Deszyfrowanie DES	88
12.6.2.9. Modyfikacje DES	88
12.6.2.10. Sieci Feistela	88
12.6.3. Algorytm AES	89
12.6.3.1. Tworzenie kluczy	89
12.6.3.2. Runda algorytmu AES	90
12.6.3.3. Bezpieczeństwo algorytmu AES	90
12.6.4. Algorytm TWOFISH	90
12.6.5. Algorytm CAST5	91
12.6.6. Algorytm RC2	91
12.6.7. Algorytm RC5	91
12.6.8. Inne wybrane symetryczne algorytmy blokowe	92
12.7. Algorytmy z kluczem publicznym	92
12.7.1. Algorytm Diffiego-Hellmana	92
12.7.2. Algorytm RSA	93
12.7.2.1. Działania systemu RSA	94
12.7.2.2. Przykładowe szyfrowanie i deszyfrowanie RSA	94
12.7.2.3. Implementacja RSA	94
12.7.3. Algorytm ElGamala	97
12.7.4. Inne wybrane algorytmy asymetryczne	98
13. Protokoły komunikacyjne podwyższające bezpieczeństwo informacji w sieciach	99
13.1. Konstrukcja wirtualnych sieci prywatnych VPN	101
13.1.1. Rodzaje i klasyfikacja sieci VPN	103
13.1.2. Klasyfikacje sieci VPN	104
13.2. Protokół IPSEC	107
13.2.1. Architektura. Zasada działania	107
13.2.2. Protokoły bezpieczeństwa IPsec	110
13.2.2.1. Protokół AH	110
13.2.2.2. Protokół ESP	111
13.2.3. Rozwój i przyszłość IPsec	112
13.2.4. SSTP jako przykład kontrtechnologii dla IPsec	113
13.2.4.1. Architektura. Zasada działania	113
13.2.5. Podsumowanie	114
13.3. Protokoły SSL/TLS	114
13.3.1. Zasada działania SSL	114
13.3.2. Zasada działania TLS	118

13.3.3.	Dodatkowe informacje o bezpieczeństwie SSL i TLS	121
13.3.4.	Porównanie protokołów SSL v2, SSL v3 i TLS	121
13.3.5.	Możliwe problemy protokołów SSL oraz TLS	122
13.3.5.1.	<i>Problemy z protokołem SSL v2</i>	122
13.3.5.2.	<i>Rozpowszechnienie TLS</i>	122
13.4.	Inne protokoły bezpiecznej komunikacji. Protokół SSH	123
13.4.1.	Architektura i zasada działania SSH	123
13.4.2.	Bezpieczeństwo SSH	124
14.	Zaawansowane metody potwierdzania tożsamości użytkownika	127
14.1.	Zastosowanie standardu OpenID w zarządzaniu	128
14.2.	Sprzętowe metody potwierdzania tożsamości użytkownika	132
14.2.1.	Działanie klucza sprzętowego YubiKey	132
14.2.2.	Klucze sprzętowe realizowane w oparciu o standard iButton	133
14.2.3.	Użycie standardu NFC na potrzeby uwierzytelniania	134
14.2.4.	Potwierdzenie tożsamości użytkownika za pomocą sieci GSM	136
14.3.	Dalszy rozwój rozwiązań OpenID	138
15.	Platforma ePUAP i profil zaufany w potwierdzaniu tożsamości użytkowników i podpisywaniu dokumentów elektronicznych	139
15.1.	Integracja systemów zewnętrznych z platformą ePUAP	142
15.2.	Wymiana danych za pomocą protokołu SAML	144
15.3.	Komunikacja systemów zewnętrznych z platformą ePUAP	147
15.3.1.	Modele komunikacji	148
15.4.	Popularyzacja i wykorzystanie profilu zaufanego	150
16.	Kryptografia w zastosowaniu do podpisu cyfrowego i identyfikacji użytkownika w sieci Internet	153
16.1.	Wprowadzenie	153
16.2.	Rozwój metod uwierzytelniania użytkownika sieci	154
16.3.	Podpis elektroniczny oparty o symetryczne algorytmy kryptografii	154
16.4.	Podpis elektroniczny oparty o niesymetryczne algorytmy kryptografii	156
16.5.	Podpis cyfrowy – rozwiązania i przepisy prawne	157
16.5.1.	Pojęcie podpisu cyfrowego	157
16.5.2.	Funkcje podpisu cyfrowego	159
16.5.2.1.	<i>UWIERZYTELNIANIE</i>	159
16.5.2.2.	<i>NIEZAPRZECZALNOŚĆ</i>	160
16.5.2.3.	<i>INTEGRALNOŚĆ</i>	160
16.5.2.4.	<i>IDENTYFIKACJA</i>	161
16.5.2.5.	<i>POUFNOŚĆ</i>	161
16.5.3.	Jednokierunkowa funkcja skrótu	161
16.5.4.	Tworzenie i weryfikacja podpisu cyfrowego	163
16.5.5.	Dystrybucja klucza	166
16.5.6.	Certyfikaty	167
16.5.7.	Centra certyfikacji i ośrodki rejestracyjne	168

16.5.8. Zarządzanie kluczami i certyfikatami	169
16.5.8.1. FAZA INICJUJĄCA	170
16.5.8.2. FAZA WYDAWANIA	172
16.5.8.3. FAZA UNIEWAŻNIANIA	173
16.5.9. Weryfikacja certyfikatów	174
16.5.10. Unieważnianie certyfikatów	175
16.5.11. Modele zaufania	176
16.5.11.1. Model hierarchiczny	176
16.5.11.2. Model zaufania skoncentrowany na użytkowniku	177
16.5.12. Przepisy prawne	179
16.6. Zaawansowane metody uwierzytelniania użytkownika	183
17. Systemy bezpieczeństwa poczty PGP	187
17.1. Historia PGP	187
17.1.1. Gnu Privacy Guard GPG	189
17.2. Działanie i bezpieczeństwo PGP	189
17.3. Narzędzia umożliwiające pracę z PGP i GPG	193
17.4. Przekazywanie kluczy na potrzeby PGP	195
17.5. Zalety wykorzystania PGP w ochronie poczty elektronicznej	196
18. Matematyczne podstawy informatyki kwantowej	197
18.1. Wprowadzenie	197
18.2. Qubity	200
18.2.1. Notacja Diraca	200
18.2.2. Qubity w zapisie wektorowym	204
18.2.3. Macierze gęstości	210
18.2.4. Stany kwantowe splątane	214
18.2.4.1. <i>Observable</i>	216
18.3. Bramki kwantowe	218
18.3.1. Bramki 1-qubitowe	218
18.3.2. Bramki 2-qubitowe	223
18.3.3. Bramki n-qubitowe	226
18.4. Perspektywiczny uniwersalny komputer kwantowy	232
18.5. Algorytmy kwantowe	233
18.5.1. Algorytm poszukiwań Grovera	234
18.5.2. Algorytm faktoryzacji Shora	240
18.5.3. Kwantowa transformacja Fouriera	242
19. Kryptografia kwantowa	247
19.1. Wprowadzenie	247
19.2. Protokoły kwantowe	248
19.2.1. Protokół BB84	250
19.2.2. Protokół B92	252
19.2.3. Protokół teleportacji kwantowej	252
19.2.3.1. <i>Stany Bella</i>	254

19.2.3.2. Wytwarzanie stanów splątanych	255
19.2.4. Qubitowy współczynnik błędu (QBER – Quantum Bit Error Rate)	257
19.2.5. Kwantowa korekcja błędów	259
20. Zastosowanie kryptografii kwantowej w sieciach komputerowych	261
20.1. Charakterystyka kwantowej dystrybucji kluczy (QKD) w sieciach	261
20.1.1. Interfejsy kwantowe	262
20.1.2. Pamięć kwantowa	263
20.1.3. Teleportacja	264
20.2. Integracja QKD z protokołami sieciowymi	264
20.2.1. Integracja QKD z warstwą 2 stosu protokołów OSI – Q3P	266
20.2.2. Integracja QKD z warstwą 3 stosu protokołów OSI – SEQKEIP	268
20.2.3. Integracja QKD z warstwą 5 stosu protokołów OSI – TSL/SSL	270
20.3. Architektura sieci QKD	271
20.3.1. Modele sieci QKD	271
20.3.1.1. Optyczne węzły QKD	272
20.3.1.2. Kwantowe węzły QKD	272
20.3.1.3. Sieć na zaufanych przekaźnikach	272
20.3.2. Topologie sieci QKD	273
20.4. Sieć kwantowa DARPA	276
20.4.1. Struktura segmentu sieci	277
20.4.1.1. System ze słabo spójnym źródłem	278
20.4.1.2. System ze stanami splątanymi	279
20.4.1.3. System komunikacji w wolnej przestrzeni	280
20.4.2. Warianty architektury	281
20.4.2.1. Wariant na przekaźnikach z pełnym zaufaniem	281
20.4.2.2. Sieć QKD na przełącznikach fotonów bez zaufania	282
20.5. Sieć wiedeńska SECOQC	282
20.5.1. Podstawowa architektura i topologia	283
20.5.2. Systemy QKD w prototypie sieci SECOQC	285
20.6. Dalszy rozwój	286
20.6.1. Platforma testowa SwissQuantum	286
20.6.2. Projekty wdrożeniowe	288
21. Przykładowe zastosowania mechanizmów ochrony informacji	289
22. Zakończenie	295
23. Spis rysunków	297
24. Spis tabel	300
25. Słownik ważniejszych skrótów i pojęć użytych w pracy	301
26. Literatura	305