

Spis treści

Od Wydawcy	8
1. Krzywe eliptyczne w kryptografii Wykorzystanie pakietu SAGE.....	9
1.1. Krzywe eliptyczne w praktyce	10
1.2. Pakiet SAGE	10
1.3. Krzywe eliptyczne na płaszczyźnie.....	10
1.4. Ciała skończone proste.....	13
1.5. Krzywe eliptyczne nad ciałami prostymi	14
1.6. Zagadnienie logarytmu dyskretnego	15
1.7. Przykład krzywej rekomendowanej przez NIST	16
1.8. Uzgadnianie klucza z wykorzystaniem krzywych eliptycznych. ECDH.....	17
1.9. Przykład ECDH na krzywej P-256.....	18
1.10. Podpis cyfrowy z wykorzystaniem krzywych eliptycznych. ECDSA	19
1.11. Przykład ECDSA na krzywej P-256	20
1.12. Moneta cyfrowa Bitcoin.....	21
12.1.1. Krzywa eliptyczna secp256k1.....	21
12.1.2. Adres Bitcoin	21
12.1.3. Bloki Bitcoin	23
1.13. Ciała skończone $GF(2^m)$	24
1.14. Krzywe eliptyczne nad ciałami binarnymi $GF(2^m)$	25
1.15. Krzywa B-283 (rekomendowana przez NIST).....	27
2. Zastosowania w kryptografii iloczynów dwuliniowych na krzywych eliptycznych.....	29
2.1. Wstęp.....	30
2.2. Protokoły oparte na iloczynach dwuliniowych	31
2.2.1. Krótkie podpisy cyfrowe.....	31
2.2.2. Uzgadnianie wspólnego klucza między trzema osobami w jednej rundzie	32
2.2.3. Kryptografia oparta na tożsamości (<i>Identity-Based Cryptography</i>)	32
2.3. Krzywe eliptyczne.....	33
2.4. Iloczyn Tate na krzywych eliptycznych	35
2.4.1. Grupa dywizorów na krzywej eliptycznej.....	36
2.4.2. Definicja iloczynu Tate i algorytm Millera	38
2.5. Metoda mnożeń zespolonych.....	39

2.6.	Konstruowanie krzywych eliptycznych z danym stopniem zanurzeniowym	43
2.7.	Rodziny parametryczne krzywych eliptycznych	46
3.	Nowy wymiar bezpieczeństwa – RSA z kluczem jednorazowym.....	55
3.1.	Wprowadzenie	56
3.2.	Szyfrowanie i klucze szyfrowania.....	57
3.2.1.	Dystrybucja kluczy symetrycznych	58
3.2.2.	Szyfrowanie asymetryczne – rozmiar kluczy RSA.....	59
3.3.	Zwiększenie bezpieczeństwa RSA.....	62
3.3.1.	Efektywność i bezpieczeństwo kryptosystemów RSA	63
3.3.2.	RSA – efektywna i bezpieczna implementacja	64
3.4.	Podsumowanie	67
4.	Problemy prawne związane z używaniem monet wirtualnych w Polsce i na świecie	69
4.1.	Zagadnienia wstępne	70
4.2.	Ogólne problemy z uregulowaniem kwestii prawnych kryptowalut typu Bitcoin	70
4.2.1.	Alternatywa wobec pieniędzy tradycyjnych	70
4.2.2.	Decentralizacja i anonimowość.....	71
4.2.3.	Granice między cyberprzestrzenią a światem rzeczywistym	72
4.3.	Wybrane szczegółowe problemy prawne związane z obrotem kryptowalutami w Polsce	72
4.3.1.	Czym jest kryptowaluta?.....	72
4.3.2.	Zobowiązania podatkowe i zaległości płatnicze	73
4.4.	Wybrane problemy prawne kryptowalut na świecie	74
4.4.1.	Pieniądz elektroniczny czy dobro wirtualne	74
4.4.2.	Giełdy, kopalnie oraz doradcy.....	75
4.5.	Podsumowanie	76
5.	Możliwości zastosowania waluty kryptograficznej Bitcoin	79
5.1.	Wprowadzenie	80
5.2.	Podstawowe definicje	80
5.2.1.	Pieniądz	80
5.2.2.	Waluta.....	80
5.2.3.	Pieniądz elektroniczny	80
5.2.4.	Podpis cyfrowy.....	81
5.2.5.	Funkcja haszująca	81
5.3.	Zasada działania systemu Bitcoin.....	81
5.4.	Pozyskiwanie monet	83

5.5.	Tendencje rozwojowe	83
5.6.	Zagrożenia	85
5.7.	Podsumowanie	85
6.	Akceleracja algorytmów kryptologicznych z wykorzystaniem struktur programowalnych.....	87
6.1.	Wstęp.....	88
6.2.	Informacje ogólne	90
6.2.1.	Systemy SoPC.....	90
6.2.2.	Sprzętowa akceleracja algorytmów.....	90
6.3.	Akceleracja szyfrów strumieniowych.....	93
6.4.	Akceleracja szyfrów blokowych.....	96
6.5.	Akceleracja kryptoanalizy szyfrów	98
6.6.	Podsumowanie	101
7.	Serwerowy system podpisu elektronicznego z uwierzytelnianiem biometrycznym	103
7.1.	Motywacja	104
7.2.	Koncepcja systemu	108
7.3.	Biometria a bezpieczeństwo	110
7.4.	Serwerowy system podpisu elektronicznego z uwierzytelnianiem biometrycznym	114
7.4.1.	Architektura systemu	115
7.4.2.	Przebieg podstawowych operacji.....	116
7.5.	Demonstracja systemu	118
7.6.	Podsumowanie	122
8.	Integracja systemów zewnętrznych z serwerową platformą operacji kryptograficznych uwierzytelnianych biometrycznie.....	125
8.1.	Wstęp.....	126
8.2.	Biometria naczyń krwionośnych palca	128
8.3.	Platforma operacji kryptograficznych uwierzytelnianych biometrycznie	132
8.4.	Implementacja standardu PKCS#11 i CryptoAPI.....	134
8.4.1.	PKCS#11	134
8.4.2.	CSP (implementacja CryptoAPI).....	137
8.5.	Prezentacja integracji aplikacji zewnętrznych z systemem operacji kryptograficznych.....	139
8.6.	Wnioski	143

9. Komercyjne zastosowania kryptografii w systemach Pay-TV	147
9.1. Wprowadzenie	148
9.2. Zabezpieczenia dostępu do treści telewizyjnych	148
9.3. Sposoby dystrybucji treści telewizyjnej	149
9.4. Rodzaje stosowanych zabezpieczeń.....	150
9.4.1. Systemy CA.....	150
9.4.2. Systemy DRM.....	152
9.4.3. Systemy zabezpieczające kanał komunikacyjny	153
9.5. Bezpieczeństwo i skuteczność systemów zabezpieczeń.....	154
9.5. Podsumowanie	155
10. Metody zabezpieczeń programów i aplikacji komputerowych	157
10.1. Wprowadzenie	158
10.2. Aktualny stan wiedzy, czyli przegląd najpopularniejszych zabezpieczeń aplikacji i programów komputerowych	158
10.2.1. Użytkownik/hasło (ang. <i>login and password</i>).....	158
10.2.2. Numer seryjny (ang. <i>serial number</i>)	159
10.2.3. Plik klucza.....	160
10.2.4. Dokuczający ekran (ang. <i>nag screen</i>)	160
10.2.5. Programy z ograniczoną funkcjonalnością (wersja demonstracyjna)	160
10.2.6. Wersja próbna z ograniczeniem czasowym (ang. <i>Trial</i>)	160
10.3. Zagrożenia zabezpieczeń programów i aplikacji komputerowych	161
10.3.1. Podatność na dekompilację	161
10.3.2. „Pułapki” na dedykowane metody interfejsu Windows, czyli słabość funkcji API	163
10.3.3. Możliwość debugowania aplikacji	164
10.3.4. Zapis danych w rejestrze Windows.....	167
10.3.5. Edycja programu bezpośrednio w pamięci	167
10.3.6. Podstawowe błędy programistyczne	167
10.4. Zaawansowane i skomplikowane zabezpieczenia programów i aplikacji – czy rzeczywiście są niezbędne?.....	168
11. Ataki na strony internetowe oraz metody zabezpieczeń	171
11.1. Wprowadzenie	172
11.2. Podstawowe definicje	172
11.3. Atak XSS	173
11.3.1. Wykorzystanie.....	173
11.3.2. Metody zabezpieczeń	174
11.3.3. Przykładowy atak	174

11.4. Atak SQLInjection	175
11.4.1. Wykorzystanie	176
11.4.2. Metody zabezpieczeń	176
11.4.3. Przykładowy atak	176
11.5. Podsumowanie	178
Prezentacje firm	179