

Wojciech Ciemski

# CYBERSECURITY

W PYTANIACH I ODPOWIEDZIACH

wydanie II



**Autor:** Wojciech Ciemski  
**Tytuł:** Cybersecurity w pytaniach i odpowiedziach  
**Wydanie:** II, rozszerzone  
**Rok wydania:** 2026  
**ISBN:** 978-83-980907-1-1  
**Projekt okładki:** Wojciech Ciemski  
**Projekt typograficzny i skład:** Wojciech Ciemski  
**Redakcja i korekta:** Wojciech Ciemski

### **Prawa autorskie**

© 2026 Wojciech Ciemski

Wszelkie prawa zastrzeżone.

Niniejsza publikacja ani żadna jej część nie może być powielana, rozpowszechniana ani przetwarzana w jakiegokolwiek formie (elektronicznej, mechanicznej, kserograficznej, nagraniowej lub innej) bez uprzedniej pisemnej zgody autora, z wyjątkiem krótkich cytatów wykorzystywanych w celach recenzji lub analizy.

### **Zastrzeżenia prawne**

Informacje zawarte w książce mają charakter edukacyjny i zostały opracowane z najwyższą starannością. Autor nie ponosi odpowiedzialności za skutki wykorzystania przedstawionych treści w praktyce.

Cyberbezpieczeństwo jest dziedziną dynamicznie rozwijającą się, dlatego część informacji może ulec dezaktualizacji wraz z rozwojem technologii oraz pojawieniem się nowych zagrożeń.

### **Znaki towarowe**

Nazwy produktów, firm i technologii użyte w książce mogą stanowić znaki towarowe lub zastrzeżone nazwy ich właścicieli. Zostały wykorzystane wyłącznie w celach informacyjnych i edukacyjnych.

### **Odpowiedzialność i użycie w praktyce**

Czytelnik wykorzystuje zawarte w książce informacje na własną odpowiedzialność. Treści mają charakter edukacyjny i nie stanowią zachęty do podejmowania nieautoryzowanych działań.

Wszelkie działania związane z testowaniem bezpieczeństwa, analizą systemów czy ingerencją w infrastrukturę IT powinny być wykonywane wyłącznie w środowiskach testowych lub za wyraźną zgodą właściciela systemu.

Nieautoryzowane działania w systemach informatycznych mogą stanowić naruszenie prawa.

### **Kontakt**

Wojciech Ciemski

Security Bez Tabu®

<https://securitybeztabu.pl>

[kontakt@securitybeztabu.pl](mailto:kontakt@securitybeztabu.pl)

*Ukochanej żonie, bez której ta książka by nie powstała.  
Za cierpliwość, wsparcie i wiarę w to, co robię – nawet wtedy, gdy sam  
miałem wątpliwości. Za wszystkie wieczory, które zamiast wspólnie  
spędzić, oddałem tej książce.*

*Moim dzieciom, małym hakerkom – żebyście kiedyś mogły zobaczyć, że  
to, co robi tata, to nie tylko komputer i klawiatura, ale pasja, upór i  
praca, która zostawia po sobie coś realnego.*

*Tacie, który zaraził mnie pasją do IT i cybersecurity.  
To od Ciebie wszystko się zaczęło – ciekawość, pierwsze pytania i chęć  
zrozumienia, jak to wszystko działa.*

# Spis Treści

|  |    |
|--|----|
| SŁOWO WSTĘPNE  | 24 |
| OD AUTORA  | 29 |
| SYSTEMY OPERACYJNE   | 32 |
| Co to jest system operacyjny i jakie są jego podstawowe funkcje?   | 32 |
| Jakie są różnice między systemami operacyjnymi Windows, Linux i macOS?   | 34 |
| Co to jest proces i wątek w kontekście systemu operacyjnego?   | 36 |
| Wyjaśnij, jak działa zarządzanie pamięcią, w tym pamięć wirtualna, stronicowanie ( <i>paging</i> ) i segmentacja w systemach operacyjnych. | 38 |
| Co to jest system plików i jakie są jego rodzaje? Porównaj NTFS, FAT32 i ext4.   | 40 |
| Jak działa mechanizm uprawnień plików w systemach Linux i Windows? Omów pojęcia takie jak SUID, SGID, sticky bit oraz ACL.                 | 41 |
| Co to jest <i>shell</i> i jakie są jej rodzaje? Jakie są podstawowe komendy systemu Linux?   | 45 |
| Co to jest <i>registry</i> w systemie Windows i jaka jest jego rola?   | 47 |
| Jak działa <i>process scheduling</i> i <i>priority management</i> w systemach operacyjnych?  | 49 |
| Wyjaśnij pojęcie <i>multithreading</i> i jak jest obsługiwane przez system operacyjny.   | 51 |
| Jak operating system zarządza urządzeniami input/output (I/O)?   | 52 |
| Wyjaśnij pojęcie <i>deadlock</i> i jak system operacyjny go unika.   | 54 |
| Co to jest <i>swap</i> i jak działa w systemie Linux?  | 55 |

|   |    |
|---|----|
| Co to jest <i>zombie process</i> w systemie Linux?  | 57 |
| Jakie są różnice między <i>user mode</i> a <i>kernel mode</i> ?   | 57 |
| Co to jest <i>journaling file system</i> i jakie ma zalety? Jak działa mechanizm <i>journaling</i> w systemach plików?  | 58 |
| Jak działa mechanizm <i>signals</i> w systemie Linux?   | 60 |
| Co to jest pamięć podręczna ( <i>cache</i> ) i jak jest zarządzana przez <i>operating system</i> ?  | 61 |
| Co to jest mechanizm <i>pipe</i> i jak jest używany w systemach Unix/Linux?   | 63 |
| Co to jest <i>bootloader</i> i jaka jest jego rola w uruchamianiu systemu operacyjnego?   | 64 |
| Co to jest <i>init system</i> w Linux i jakie są jego rodzaje ( <i>SysVinit</i> , <i>systemd</i> )?   | 65 |
| Jak działa Application Programming Interface (API) w systemie operacyjnym?  | 66 |
| Co to jest <i>kernel module</i> i jak jest ładowany w systemie Linux?   | 68 |
| Wyjaśnij pojęcie <i>kernel compilation</i> i kiedy jest to konieczne.   | 68 |
| Jak działa mechanizm obsługi przerwań w systemie operacyjnym?   | 70 |
| Jak działa mechanizm <i>virtualization</i> i <i>containerization</i> na poziomie systemu operacyjnego? Omów różnice między nimi, ich zalety i wady w kontekście bezpieczeństwa. | 72 |
| Co to jest <i>symlink</i> i <i>hard link</i> w systemach plików?  | 74 |
| Jak działa mechanizm <i>copy-on-write</i> w zarządzaniu pamięcią?   | 76 |
| Co to jest <i>process isolation</i> i dlaczego jest ważna?  | 77 |
| Jak działa mechanizm kontroli dostępu w systemach operacyjnych? Omów modele <i>MAC</i> i <i>RBAC</i> .  | 79 |
| Jak działa system kolejkowania zadań (np. <i>cron</i> , <i>Task Scheduler</i> ) w systemie operacyjnym?   | 80 |

|   |     |
|---|-----|
| Jak działa mechanizm logowania zdarzeń i przechowywania logów systemowych w systemie operacyjnym?   | 83  |
| Co to jest system plików rozproszonych?   | 84  |
| Co to jest <i>cgroups</i> i <i>namespaces</i> w systemie Linux i jakie mają zastosowanie w izolacji zasobów?  | 85  |
| Co to jest <i>sysfs</i> i <i>procfs</i> w systemie Linux?   | 87  |
| Jak działa mechanizm <i>SELinux</i> i <i>AppArmor</i> ? Porównaj je i omów ich wpływ na bezpieczeństwo systemu.                                       | 89  |
| Wyjaśnij pojęcie <i>buffer overflow</i> i jak system operacyjny może mu zapobiegać.   | 91  |
| Co to jest <i>TPM (Trusted Platform Module)</i> i jak współpracuje z systemem operacyjnym?  | 92  |
| Jak działa mechanizm <i>UEFI Secure Boot</i> i jakie ma znaczenie dla bezpieczeństwa?   | 94  |
| Wyjaśnij pojęcie <i>Full Disk Encryption</i> i jak jest realizowane na poziomie systemu. Omów mechanizmy takie jak <i>BitLocker</i> i <i>LUKS</i> .   | 95  |
| Jak działa mechanizm <i>hibernation</i> w systemach operacyjnych?   | 97  |
| Co to jest mechanizm logowania użytkowników i jak jest zarządzany przez system operacyjny? Wyjaśnij pojęcia <i>UID</i> i <i>GID</i> w systemie Linux. | 99  |
| Jak działa mechanizm <i>sudo</i> i jakie ma zastosowanie?   | 100 |
| Co to są <i>environment variables</i> i jak są używane?   | 101 |
| Co znajdziemy w plikach <i>/etc/passwd</i> i <i>/etc/shadow</i> w systemie Linux?   | 103 |
| Jak można wykorzystać programy <i>wget</i> i <i>curl</i> ?  | 104 |
| Jak w bezpieczny sposób można połączyć się z serwerem?  | 106 |
| Wyjaśnij znaczenie regularnej aktualizacji oprogramowania i systemów operacyjnych.  | 108 |
| Co to jest i jak działa <i>Active Directory (AD)</i> ?  | 109 |

|  |            |
|--|------------|
| Jakie znasz programy do wirtualizacji?   | 110        |
| Co to jest <i>Docker</i> i do czego służy?   | 112        |
| Jakie są typy <i>backupu</i> (kopii zapasowych) i jak zapewnić <i>backup</i> i odzyskiwanie danych w przypadku awarii? | 113        |
| Czym różni się <i>backup</i> od <i>archiving</i> ?   | 116        |
| Co to jest <i>LVM</i> i jakie są zalety korzystania z <i>LVM</i> ?   | 117        |
| Jakie znasz systemy plików obsługiwane przez Linux i Windows?  | 118        |
| Czym różni się konto <i>root</i> od zwykłego konta użytkownika?  | 119        |
| Gdzie kieruje adres 127.0.0.1?   | 120        |
| Jakie są najlepsze praktyki w utrzymaniu systemu oraz w zarządzaniu jego aktualizacjami?                               | 121        |
| Jakie narzędzia zastosujesz do automatyzacji zadań administracyjnych?  | 123        |
| Jakie są różnice pomiędzy <i>shell</i> a <i>reverse shell</i> ?  | 124        |
| Co to jest mechanizm <i>udev</i> w systemie Linux i jakie ma zadania?  | 125        |
| Wyjaśnij pojęcie <i>kernel panic</i> i jakie są jej przyczyny.   | 126        |
| Jak działa mechanizm odzyskiwania systemu po awarii?   | 128        |
| <b>SIECI</b>   | <b>131</b> |
| Wyjaśnij różnice między modelami OSI a TCP/IP oraz wymień warstwy modelu TCP/IP.                                       | 131        |
| Co to jest adres <i>IP</i> , z czego się składa, i jakie są różnice między <i>IPv4</i> a <i>IPv6</i> ?                 | 133        |
| Jaka jest różnica między publicznym a prywatnym adresem <i>IP</i> ? Podaj przykład prywatnego adresu <i>IP</i> .       | 134        |
| Jak działa maska podsieci i do czego służy?  | 135        |

|  |     |
|--|-----|
| Co to jest brama domyślna ( <i>default gateway</i> ) w sieciach komputerowych?   | 136 |
| Jaka jest różnica między adresem <i>IP</i> a adresem <i>MAC</i> ? Co to jest <i>MAC address</i> i jakie ma znaczenie w sieci lokalnej?   | 137 |
| Co to jest <i>NAT (Network Address Translation)</i> , jakie są jego typy i jak działa mechanizm <i>NAT Loopback</i> ?  | 139 |
| Wyjaśnij działanie protokołu <i>ARP (Address Resolution Protocol)</i> .  | 140 |
| Co to jest protokół <i>DHCP</i> , jak działa w sieci, i co to jest <i>DHCP Relay</i> ?   | 141 |
| Jak działa <i>DNS</i> i jakie jest jego znaczenie w sieciach komputerowych?  | 143 |
| Co to jest <i>VLAN</i> , do czego jest używany, co to jest <i>VLAN Trunking</i> i jakie są jego korzyści?  | 144 |
| Co to jest <i>VLAN hopping</i> i jak się przed nim zabezpieczyć?   | 146 |
| Co to jest segmentacja sieci i jakie ma znaczenie dla bezpieczeństwa?  | 147 |
| Co to jest przełącznik ( <i>switch</i> ), jak działa, czym różni się od koncentratora ( <i>hub</i> ) i jaka jest różnica pomiędzy routerem a <i>switchem</i> ?                                 | 149 |
| Co to jest router i jaka jest jego rola w sieci?   | 150 |
| Jakie urządzenia wykorzystuje się do budowania sieci i jakie są ich funkcje?   | 151 |
| Wyjaśnij różnice między siecią <i>LAN</i> , <i>MAN</i> i <i>WAN</i> .  | 153 |
| Co to jest topologia sieci i jakie są jej rodzaje? Jakie znasz topologie sieci i architektury sieciowe?  | 154 |
| Jak działa protokół <i>TCP</i> , jakie ma cechy charakterystyczne i co to jest trójfazowe uzgadnianie połączenia ( <i>Three-way handshake</i> )?   | 156 |
| Co to jest protokół <i>UDP</i> i kiedy jest używany zamiast <i>TCP</i> ?   | 158 |
| Co to jest <i>firewall</i> , jakie są jego rodzaje i jakie są różnice między <i>firewallem</i> sprzętowym a programowym? Jaka jest różnica między rozwiązaniami <i>firewall</i> a <i>WAF</i> ? | 159 |

|  |     |
|--|-----|
| Co to jest DMZ (Demilitarized Zone) w kontekście sieci komputerowych?  | 160 |
| Wyjaśnij pojęcie ataków sieciowych takich jak <i>DoS/DDoS</i> , <i>Man-in-the-Middle</i> , <i>ARP Poisoning</i> , <i>DNS Spoofing</i> , <i>Smurf Attack</i> , <i>MAC Flooding</i> , <i>VLAN Hopping</i> i jak się przed nimi bronić. | 161 |
| Jak działa protokół <i>SSL/TLS</i> w zabezpieczeniu komunikacji sieciowej?   | 164 |
| Co to jest <i>VPN</i> , jakie są jego zastosowania i jakie technologie <i>VPN</i> oraz bezpieczeństwa sieci znasz?   | 166 |
| Wyjaśnij działanie protokołu <i>IPsec</i> .  | 168 |
| Jak działa protokół <i>SSH</i> i jakie ma zastosowanie w sieciach?   | 169 |
| Co to jest protokół <i>FTP</i> , jakie są jego bezpieczne alternatywy i jakie zalety ma <i>SFTP</i> nad <i>FTP</i> ? Czy <i>FTP</i> jest bezpieczniejsze niż <i>SSH</i> ?  | 170 |
| Wyjaśnij działanie protokołu <i>HTTP</i> i różnice między <i>HTTP</i> a <i>HTTPS</i> .   | 171 |
| Wyjaśnij różnice między protokołami zabezpieczeń sieci <i>Wi-Fi</i> : <i>WEP</i> , <i>WPA</i> i <i>WPA2</i> . Czy w sieciach bezprzewodowych powinno się korzystać z <i>WEP</i> ?  | 172 |
| Co to jest sieć bezprzewodowa i jakie są jej standardy (np. <i>802.11a/b/g/n/ac</i> )?   | 173 |
| Co to jest <i>SSID</i> i jakie ma znaczenie w sieciach <i>Wi-Fi</i> ?  | 175 |
| Co to jest adresowanie statyczne i dynamiczne w sieciach <i>IP</i> ?   | 176 |
| Wyjaśnij pojęcie <i>QoS (Quality of Service)</i> i jego znaczenie w sieciach.  | 177 |
| Jak działa <i>load balancing</i> w sieciach komputerowych?   | 178 |
| Co to jest sieć peer-to-peer ( <i>P2P</i> ) i sieć klient-serwer? Jakie są ich cechy?  | 179 |
| Co to jest <i>multicast</i> i jakie ma zastosowanie?   | 180 |
| Jak działa protokół <i>STP (Spanning Tree Protocol)</i> i do czego służy?  | 182 |
| Wyjaśnij pojęcie <i>port security</i> na przełącznikach sieciowych.  | 184 |
| Jak działa technologia <i>Power over Ethernet (PoE)</i> ?  | 185 |

Co to jest sieć definiowana programowo (*Software Defined Network, SDN*) i jakie ma zalety? 186

Wyjaśnij pojęcie sieci rozległej (*Wide Area Network, WAN*) i technologie jej realizacji. 187

Jak działa protokół *Voice over Internet Protocol (VoIP)* i jakie są jego wymagania sieciowe? 189

Wyjaśnij działanie protokołu *Network Time Protocol (NTP)* i jego znaczenie w sieciach. 191

Jak działa protokół *Open Shortest Path First (OSPF)* i jakie są jego zalety? 192

Wyjaśnij pojęcie *Maximum Transmission Unit (MTU)* i jego wpływ na sieć. 194

## APLIKACJE WEBOWE 196

Co to jest aplikacja webowa, jak różni się od tradycyjnej aplikacji desktopowej i strony internetowej? Jakie narzędzia są używane do jej tworzenia? 196

Jak działa model klient-serwer w kontekście aplikacji webowych? 197

Co to jest protokół *HTTP* i jakie są jego główne metody (*GET, POST, PUT, DELETE, etc.*)? Jaka jest różnica między metodami *GET* i *POST*? 199

Wyjaśnij różnicę między *HTTP* a *HTTPS* pod względem funkcjonalności. 200

Co to jest przeglądarka internetowa i jaka jest jej rola w działaniu aplikacji webowych? 201

Jakie są podstawowe technologie używane do tworzenia frontendu aplikacji webowych? 202

Co to jest *HTML*, jakie są jego podstawowe elementy i wymień najważniejsze tagi języka *HTML*. 204

Jak działa *CSS* i do czego jest używany w aplikacjach webowych? 206

Wyjaśnij pojęcie *DOM (Document Object Model)* i jego znaczenie w manipulacji stroną. 207

|  |     |
|--|-----|
| Co to są <i>frontend frameworks</i> i podaj przykłady (np. <i>React</i> , <i>Angular</i> , <i>Vue.js</i> ).<br>Jakie technologie stosuje się do tworzenia interaktywnych interfejsów<br>użytkownika ( <i>User Interface, UI</i> )? | 208 |
| Co to są <i>backend frameworks</i> i podaj przykłady.  | 210 |
| Wyjaśnij pojęcie <i>RESTful API</i> , jego znaczenie w komunikacji między aplikacjami<br>i jakie technologie są stosowane w tworzeniu aplikacji opartych o <i>REST API</i> .   | 211 |
| Co to jest <i>JSON</i> , jakie ma zastosowanie w wymianie danych i jak wygląda<br>przykładowy plik w formacie <i>JSON</i> ?  | 212 |
| Co to jest <i>Single Page Application (SPA)</i> i jakie są jego wady i zalety?   | 214 |
| Jak działa <i>routing</i> w aplikacjach webowych?  | 215 |
| Co to jest <i>Progressive Web App (PWA)</i> i jakie korzyści przynosi użytkownikom?  | 216 |
| Co to jest <i>WebSocket</i> i jak umożliwia komunikację w czasie rzeczywistym?   | 217 |
| Jak działa mechanizm lokalnego przechowywania danych w przeglądarce?   | 219 |
| Co to jest <i>CDN (Content Delivery Network)</i> i jak wpływa na wydajność aplikacji?  | 221 |
| Co to jest <i>middleware</i> w kontekście frameworków backendowych?  | 221 |
| Wyjaśnij pojęcie <i>ORM (Object-Relational Mapping)</i> i jego zastosowanie.   | 222 |
| Co to jest baza danych, jakie są rodzaje baz danych używanych w aplikacjach<br>webowych ( <i>SQL vs NoSQL</i> ) i jakie typy danych są w nich przechowywane i<br>przetwarzane?   | 224 |
| Jak działa komunikacja między <i>frontendem</i> a <i>backendem</i> w aplikacji webowej?  | 226 |
| Co to jest <i>API</i> , jakie są jego typy ( <i>REST, GraphQL, SOAP</i> ) i jak przebiega<br>integracja <i>API</i> z aplikacjami?  | 228 |

|  |     |
|--|-----|
| Wyjaśnij różnice między serwerem dedykowanym a chmurą w kontekście hostowania aplikacji. | 230 |
| Co to jest <i>Server-Side Rendering</i> (SSR) i jakie są jego zalety?                    | 232 |
| Wyjaśnij pojęcie <i>Client-Side Rendering</i> (CSR) i kiedy jest stosowane.              | 233 |
| Co to jest <i>HTTP/2</i> i jakie korzyści przynosi w porównaniu do <i>HTTP/1.1</i> ?     | 234 |
| Jak działa mechanizm cache'owania w aplikacjach webowych?                                | 235 |
| Jakie znasz kody i klasy odpowiedzi <i>HTTP</i> ?  | 237 |
| Co to są <i>microservices</i> i jakie są ich zalety w architekturze aplikacji?           | 238 |
| Wyjaśnij pojęcie architektury monolitycznej w kontekście aplikacji webowych.             | 239 |
| Co to jest <i>GraphQL</i> i jak różni się od tradycyjnych API <i>REST</i> ?              | 241 |
| Jak działa mechanizm <i>drag and drop</i> w <i>HTML5</i> ?                               | 242 |
| Wyjaśnij pojęcie <i>Service Workers</i> w kontekście <i>PWA</i> .                        | 244 |
| Wyjaśnij różnice między protokołami <i>HTTP</i> i <i>WebSocket</i> .                     | 245 |
| Jak działa mechanizm geolokalizacji w przeglądarkach?                                    | 246 |
| Co to jest <i>MIME type</i> i jakie ma znaczenie w przesyłaniu danych?                   | 247 |
| Co to są atrybuty <i>data-</i> w <i>HTML5</i> i jak są używane?                          | 248 |
| Jak działa mechanizm <i>lazy loading</i> obrazów i treści?                               | 250 |
| Co to jest <i>virtual DOM</i> i jakie są jego zalety w frameworkach frontendowych?       | 251 |
| Co to jest <i>TypeScript</i> i jakie korzyści przynosi w tworzeniu aplikacji webowych?   | 252 |
| Jak działa JavaScript bundler (np. <i>Webpack</i> , <i>Rollup</i> )?                     | 253 |
| Co to jest <i>transpiler</i> i jakie narzędzia są używane (np. <i>Babel</i> )?           | 255 |

|   |            |
|---|------------|
| Wyjaśnij pojęcie <i>polyfill</i> i kiedy jest potrzebny.  | 256        |
| Co to jest <i>IndexedDB</i> i do czego służy w aplikacjach webowych?  | 257        |
| Jak działa mechanizm <i>client-side routing</i> w <i>SPA</i> ?  | 259        |
| Wyjaśnij pojęcie <i>hydration</i> w kontekście <i>SSR</i> .   | 260        |
| Co to jest <i>JAMstack</i> i jakie są jego główne komponenty?   | 261        |
| O czym informuje zawartość nagłówka <i>User-Agent</i> ?   | 262        |
| Co oznacza, że <i>HTTP</i> jest protokołem bezstanowym?   | 263        |
| Przed czym chroni <i>CSP</i> ?  | 264        |
| Czy powinno się ustawiać flagę <i>HttpOnly/Secure</i> w <i>cookies</i> i dlaczego tak lub nie?  | 265        |
| Do czego wykorzystuje się protokół <i>WebSocket</i> ?   | 266        |
| Jakie są różnice między serwerami <i>Apache</i> i <i>Nginx</i> w kontekście hostowania aplikacji webowych?  | 267        |
| <b>KRYPTOGRAFIA</b>   | <b>269</b> |
| Co to jest kryptografia, jakie są jej główne cele i podstawowe zasady?  | 269        |
| Wyjaśnij różnicę między kryptografią symetryczną a asymetryczną i ich zastosowania.   | 270        |
| Co to jest klucz kryptograficzny, jakie są jego rodzaje i jak zarządzać kluczami?   | 272        |
| Jak działa algorytm <i>AES</i> , czym jest szyfrowanie blokowe ( <i>block cipher</i> ) i jakie są tryby jego pracy ( <i>ECB</i> , <i>CBC</i> itp.)?                 | 274        |
| Co to jest <i>RSA</i> i jak działa ten algorytm?  | 276        |
| Wyjaśnij pojęcie funkcji skrótu ( <i>hash function</i> ), jakie są jej zastosowania oraz różnice między <i>MD5</i> , <i>SHA-1</i> , <i>SHA-256</i> i <i>SHA-3</i> . | 277        |

|  |     |
|--|-----|
| Jakie są zagrożenia związane z używaniem słabych funkcji skrótu i co to jest atak kolizyjny?   | 279 |
| Co to jest podpis cyfrowy i jak działają algorytmy DSA, ECDSA i ElGamal?   | 280 |
| Jak działają algorytmy DSA, ECDSA i ElGamal?   | 281 |
| Jak działa protokół <i>SSL/TLS</i> w zabezpieczaniu komunikacji, czym jest <i>handshake</i> i jakie ulepszenia wprowadza <i>TLS 1.3</i> ?  | 283 |
| Wyjaśnij pojęcie certyfikatu cyfrowego, jego rolę, typy ( <i>EV SSL, wildcard, self-signed, root CA</i> ) oraz znaczenie <i>certificate pinning</i> .  | 284 |
| Co to jest infrastruktura klucza publicznego ( <i>Public Key Infrastructure, PKI</i> ) i jak działa?   | 286 |
| Wyjaśnij pojęcie losowości ( <i>randomness</i> ), entropii ( <i>entropy</i> ) i generatorów liczb pseudolosowych ( <i>Pseudorandom Number Generators, PRNG</i> ) w kryptografii.   | 287 |
| Co to jest atak kryptograficzny ( <i>cryptographic attack</i> ), jakie są jego typy ( <i>brute force, man-in-the-middle, replay, side-channel, padding oracle, chosen-plaintext, collision attack</i> ) i jak się przed nimi bronić? | 289 |
| Co to jest kryptografia kwantowa ( <i>quantum cryptography</i> ) i kryptografia postkwantowa ( <i>post-quantum cryptography</i> ), jakie są ich potencjalne zastosowania?  | 291 |
| Jak działa algorytm Diffie-Hellman, protokół <i>ECDH</i> i czym jest grupa Diffie-Hellmana?  | 292 |
| Wyjaśnij pojęcie <i>salting</i> i <i>peppering</i> haseł, <i>hash stretching</i> , funkcji <i>KDF</i> (np. <i>PBKDF2</i> ) i dlaczego są ważne.  | 295 |
| Co to jest HMAC (Hash-Based Message Authentication Code) i jak działa?   | 296 |
| Co to jest <i>steganography</i> i jak się różni od <i>cryptography</i> ?   | 297 |
| Jak działa mechanizm <i>Perfect Forward Secrecy (PFS)</i> w protokołach kryptograficznych?   | 298 |
| Co to jest algorytm szyfrowania <i>RC4 (Rivest Cipher 4)</i> i dlaczego nie jest już zalecany?   | 299 |

|  |     |
|--|-----|
| Jak działa protokół PGP (Pretty Good Privacy)?   | 300 |
| Co to jest HSM (Hardware Security Module) i do czego służy?  | 301 |
| Jak działa protokół <i>Kerberos</i> w kontekście kryptografii?   | 303 |
| Co to jest zasada Kerckhoffs'a i jakie ma znaczenie w projektowaniu systemów kryptograficznych?                                  | 304 |
| Jak działa mechanizm szyfrowania <i>end-to-end</i> w komunikatorach?   | 305 |
| Jak działa protokół <i>IPsec</i> w kontekście kryptografii?  | 306 |
| Jak działają tokeny <i>U2F</i> i co nam daje wykorzystanie <i>2FA</i> ?  | 307 |
| Jakie techniki kryptograficzne są stosowane w <i>Blockchain</i> i jakie są ich zalety i wady w kontekście bezpieczeństwa danych? | 308 |
| Jakie są najważniejsze protokoły kryptograficzne stosowane w sieciach komputerowych?   | 311 |
| Wytłumacz, jak działa kryptografia wieloczynnikowa.  | 313 |
| Wyjaśnij różnicę między hashowaniem a szyfrowaniem.  | 314 |
| Co to jest algorytm szyfrowania ChaCha20 i jakie ma zastosowania?  | 315 |
| <b>CYBERBEZPIECZEŃSTWO</b>   | 316 |
| Co to jest bezpieczeństwo informacji i jakie są jego główne cele?  | 316 |
| Wyjaśnij triadę CIA (Confidentiality, Integrity, Availability).  | 316 |
| Co oznacza autentyczność i nieodrzucałość w kontekście bezpieczeństwa informacji?  | 317 |
| Jakie są podstawowe zagrożenia i podatności dla bezpieczeństwa informacji?   | 318 |
| Wyjaśnij różnicę między podatnością (vulnerability) a zagrożeniem (threat).  | 318 |

Wyjaśnij różnicę między bezpieczeństwem informacji (bezpieczeństwo informacji) a bezpieczeństwem cybernetycznym (cyberbezpieczeństwo).319

Co to jest ryzyko (risk) w bezpieczeństwie informacji i jak je oceniać? 319

Jakie są główne zasady ochrony danych osobowych i regulacje (np. GDPR)? 320

Co to jest polityka bezpieczeństwa informacji (bezpieczeństwo informacji policy) i jakie elementy powinna zawierać? 322

Jakie są role i odpowiedzialności w zarządzaniu bezpieczeństwem informacji (bezpieczeństwo informacji management)? 323

Wyjaśnij znaczenie edukacji i świadomości bezpieczeństwa (security education and awareness) w organizacji. 324

Co to jest incydent bezpieczeństwa (security incident) i jak powinno się na niego reagować? 325

Jakie są podstawowe metody uwierzytelniania użytkowników (user authentication methods) i czym różni się autoryzacja (authorization) od uwierzytelniania (authentication)? 326

Jakie są różnice między atakami pasywnymi (passive attacks) a aktywnymi (active attacks)? 327

Co to jest bezpieczeństwo fizyczne (physical security) i jakie ma znaczenie dla ochrony informacji? 327

Jakie są standardy i normy związane z bezpieczeństwem informacji (bezpieczeństwo informacji standards and norms)? 328

Co to jest bezpieczeństwo aplikacji (application security) i dlaczego jest ważne? 329

Wyjaśnij rolę kryptografii (cryptography) w bezpieczeństwie informacji.330

Co to jest zarządzanie ryzykiem (risk management) w kontekście bezpieczeństwa informacji i jakie są jego główne etapy? 331

Jakie są strategie reagowania na ryzyko (risk response strategies)? 332

|  |            |
|--|------------|
| <b>Co to jest apetyt na ryzyko (risk appetite) i jak wpływa na decyzje organizacji?</b>  | <b>333</b> |
| <b>Jak tworzy się matrycę ryzyka (risk matrix) i do czego służy?</b>   | <b>333</b> |
| <b>Co to jest plan ciągłości działania (Business Continuity Plan, BCP) i jak różni się od polityki bezpieczeństwa (security policy)?</b> | <b>334</b> |
| <b>Co to jest uwierzytelnianie wieloskładnikowe (Multi-Factor Authentication, MFA) i dlaczego jest ważne?</b>                            | <b>335</b> |
| <b>Co to jest zarządzanie tożsamością i dostępem (Identity and Access Management, IAM) i jakie są jego główne komponenty?</b>            | <b>336</b> |
| <b>Wyjaśnij kontrolę dostępu opartą na rolach (Role-Based Access Control, RBAC) i atrybutach (Attribute-Based Access Control, ABAC).</b> | <b>337</b> |
| <b>Co to jest Single Sign-On (SSO) i jakie są jego zalety?</b>   | <b>338</b> |
| <b>Jakie są wyzwania w zarządzaniu uprawnieniami użytkowników?</b>   | <b>339</b> |
| <b>Co to jest identity federation i jakie ma zastosowanie?</b>   | <b>340</b> |
| <b>Jakie są best practices w zarządzaniu aktualizacjami systemu operacyjnego?</b>  | <b>340</b> |
| <b>Co to jest operating system hardening i jakie są jego etapy?</b>  | <b>342</b> |
| <b>Jakie są metody zabezpieczania kont użytkowników w systemie?</b>  | <b>343</b> |
| <b>Co to jest mechanizm kontroli dostępu (Access Control) w systemach operacyjnych?</b>  | <b>344</b> |
| <b>Jakie są zagrożenia związane z niewłaściwą konfiguracją systemu operacyjnego?</b>   | <b>345</b> |
| <b>Wyjaśnij pojęcie SQL Injection i jak można się przed nim bronić.</b>  | <b>346</b> |
| <b>Co to jest Cross-Site Scripting (XSS) i jakie są metody jego zapobiegania?</b>  | <b>347</b> |
| <b>Jakie są najlepsze praktyki w bezpiecznym programowaniu?</b>  | <b>348</b> |
| <b>Co to jest test penetracyjny aplikacji i jakie są jego etapy?</b>   | <b>349</b> |

|  |     |
|--|-----|
| Jakie narzędzia są używane do analizy bezpieczeństwa kodu źródłowego?                      | 350 |
| Co to jest bezpieczeństwo API i jakie są jego kluczowe elementy?                           | 351 |
| Jakie są różnice między testami statycznymi a dynamicznymi bezpieczeństwa aplikacji?       | 352 |
| Co to jest deserializacja niebezpiecznych danych i jak wpływa na bezpieczeństwo aplikacji? | 353 |
| Jakie są zagrożenia związane z używaniem zewnętrznych bibliotek i jak je minimalizować?    | 354 |
| Co to jest DevSecOps i jak wpływa na bezpieczeństwo aplikacji?                             | 354 |
| Jakie są metody ochrony danych w aplikacjach?  | 355 |
| Jak tworzyć i wdrażać polityki bezpieczeństwa w organizacji?                               | 356 |
| Jak często powinno się aktualizować polityki i procedury bezpieczeństwa?                   | 357 |
| Co to jest firewall i jakie są jego typy?  | 358 |
| Jak działają systemy wykrywania i zapobiegania włamaniom (IDS/IPS)?                        | 359 |
| Co to jest segmentacja sieci i jakie korzyści przynosi?                                    | 360 |
| Jakie są najlepsze praktyki w konfiguracji sieci bezprzewodowych?                          | 360 |
| Co to jest VPN i jak wpływa na bezpieczeństwo sieci?                                       | 361 |
| Co to jest atak typu Man-in-the-Middle i jak się przed nim bronić?                         | 362 |
| Jakie są metody szyfrowania komunikacji sieciowej?   | 362 |
| Co to jest protokół SSL/TLS i jakie ma znaczenie dla bezpieczeństwa?                       | 363 |
| Co to jest atak DDoS i jakie są metody obrony przed nim?                                   | 364 |
| Co to jest honeypot i jakie ma zastosowanie w bezpieczeństwie sieci?                       | 365 |
| Jakie są metody szyfrowania danych na dyskach i w bazach danych?                           | 365 |

|  |     |
|--|-----|
| Jakie są zasady minimalizacji danych i dlaczego są ważne?                        | 366 |
| Co to jest anonimizacja i pseudonimizacja danych?                                | 367 |
| Jakie są obowiązki firmy w przypadku naruszenia ochrony danych osobowych?        | 367 |
| Co to jest Privacy by Design i jak się ją implementuje?                          | 368 |
| Co to jest Data Loss Prevention (DLP) i jakie są jego funkcje?                   | 369 |
| Co to jest złośliwe oprogramowanie (malware) i jakie są jego rodzaje?            | 370 |
| Jak działa oprogramowanie antywirusowe i jakie są jego funkcje?                  | 371 |
| Co to jest phishing i jak się przed nim bronić?                                  | 372 |
| Co to jest atak typu zero-day i jak można się przed nim zabezpieczyć?            | 373 |
| Co to jest botnet i jakie zagrożenia ze sobą niesie?                             | 374 |
| Jakie są etapy procesu reagowania na incydenty bezpieczeństwa?                   | 374 |
| Jakie są metody wykrywania incydentów bezpieczeństwa?                            | 375 |
| Co to jest test penetracyjny i jakie są jego cele?                               | 377 |
| Jakie są różnice między testem penetracyjnym a skanowaniem podatności?           | 377 |
| Jakie są etyczne i legalne aspekty testów penetracyjnych?                        | 378 |
| Jakie narzędzia są powszechnie używane w testach penetracyjnych?                 | 379 |
| Co to jest Metasploit i jakie ma zastosowanie?                                   | 380 |
| Co to jest chmura obliczeniowa i jakie są jej modele usług (IaaS, PaaS, SaaS)?   | 381 |
| Jakie są główne zagrożenia bezpieczeństwa w chmurze?                             | 382 |
| Co to jest model współodpowiedzialności (Shared Responsibility Model) w chmurze? | 383 |

|   |     |
|---|-----|
| Jakie są metody szyfrowania danych w chmurze?   | 384 |
| Co to jest bezpieczeństwo aplikacji mobilnych i dlaczego jest ważne?                            | 385 |
| Jakie są najczęstsze zagrożenia dla aplikacji mobilnych według OWASP Mobile Top 10?             | 386 |
| Jakie są metody zabezpieczania komunikacji na urządzeniach mobilnych?                           | 388 |
| Co to jest BYOD (Bring Your Own Device) i jakie są wyzwania z nim związane?                     | 389 |
| Jakie są metody ochrony danych na wypadek utraty lub kradzieży urządzenia?                      | 390 |
| Jakie są podstawowe elementy systemu bezpieczeństwa fizycznego?                                 | 391 |
| Co to jest system SIEM i jakie są jego funkcje?   | 391 |
| Jakie są najlepsze praktyki w monitorowaniu i analizie logów systemowych?                       | 392 |
| Co to jest audyt wewnętrzny i zewnętrzny w obszarze bezpieczeństwa?                             | 393 |
| Jakie są etapy procesu audytu bezpieczeństwa informacji?  | 394 |
| Co powinien zawierać raport z audytu bezpieczeństwa?  | 395 |
| Co to jest zgodność w kontekście bezpieczeństwa informacji?                                     | 395 |
| Jakie są główne regulacje prawne dotyczące ochrony danych?                                      | 396 |
| Jak sztuczna inteligencja wpływa na cyberbezpieczeństwo – zarówno pozytywnie, jak i negatywnie? | 396 |
| Co to jest supply chain attack i jakie są przykłady?  | 397 |
| Co to jest zero trust security model i dlaczego zyskuje na popularności?                        | 398 |
| Jakie są zagrożenia związane z pracą zdalną i jak organizacje mogą się przed nimi chronić?      | 399 |
| Co to jest quantum computing i jakie wyzwania stawia przed kryptografią?                        | 400 |

|   |     |
|---|-----|
| Jakie są nowe techniki ataków socjotechnicznych?                                      | 401 |
| Co to jest DevOps i jakie są jego główne założenia?                                   | 402 |
| Jakie są kluczowe elementy DevSecOps i jak różni się od DevOps?                       | 402 |
| Jak integracja bezpieczeństwa w procesie CI/CD wpływa na jakość oprogramowania?       | 403 |
| Co to jest shift-left w kontekście bezpieczeństwa i dlaczego jest ważne?              | 404 |
| Jakie są metody zarządzania tajnymi danymi (secrets) w CI/CD pipelines?               | 404 |
| Jakie są najlepsze praktyki w zabezpieczaniu kontenerów i środowisk Kubernetes?       | 405 |
| Co to jest CSIRT i jakie są jego zadania?   | 407 |
| Co to jest wirtualizacja i jakie są jej główne rodzaje?                               | 407 |
| Jakie są najlepsze praktyki w zabezpieczaniu środowisk wirtualnych i kontenerowych?   | 408 |
| Jakie są metody monitorowania bezpieczeństwa w środowiskach wirtualnych?              | 410 |
| Co to jest Kubernetes i jakie są jego mechanizmy bezpieczeństwa?                      | 410 |
| Co to jest inżynieria społeczna (social engineering) i jakie są jej główne techniki?  | 412 |
| Co to jest atak typu CEO Fraud i jak go rozpoznać?                                    | 413 |
| Jakie są najczęstsze podatności w aplikacjach webowych według OWASP Top 10?           | 414 |
| Jakie są najlepsze praktyki w zarządzaniu sesjami użytkowników?                       | 415 |
| Jakie są metody walidacji i sanitizacji danych wejściowych?                           | 416 |
| Co to jest Insecure Direct Object References (IDOR) i jak im zapobiegać?              | 417 |
| Jakie narzędzia są używane do analizy i testowania bezpieczeństwa aplikacji webowych? | 418 |

|  |     |
|--|-----|
| Co to jest inteligencja o zagrożeniach (Threat Intelligence (analiza zagrożeń)) i jakie ma znaczenie dla bezpieczeństwa organizacji? | 419 |
| Jakie są główne źródła informacji o zagrożeniach?  | 419 |
| Co to jest modelowanie zagrożeń i jakie są jego etapy?   | 420 |
| Jakie są różnice między taktyczną, operacyjną i strategiczną inteligencją o zagrożeniach?  | 422 |
| Jakie są metody analizy zachowania atakujących?  | 422 |
| Co to jest MITRE ATT&CK Framework i jak jest używany w analizie zagrożeń?  | 424 |
| Jakie są korzyści z integracji Threat Intelligence (analiza zagrożeń) z systemami bezpieczeństwa (np. SIEM)?                         | 424 |
| Co to jest Threat Hunting i jak różni się od reaktywnego podejścia do bezpieczeństwa?  | 425 |
| Jakie są metody testowania bezpieczeństwa aplikacji mobilnych?   | 426 |
| Jakie są różnice w zabezpieczaniu aplikacji na platformach Android i iOS?  | 427 |
| Co to jest Code Obfuscation i jak pomaga w ochronie aplikacji mobilnych?   | 428 |
| Co to jest Big Data i jakie wyzwania stawiają przed bezpieczeństwem?   | 429 |
| Jakie są wyzwania związane z szyfrowaniem danych w środowiskach Big Data?  | 429 |
| Co to jest Data Lake i jakie są jego implikacje dla bezpieczeństwa?  | 430 |
| Jakie są zagrożenia związane z integracją różnych źródeł danych?   | 431 |
| Co to jest OT Security i jak różni się od IT Security?   | 431 |
| Jakie są główne zagrożenia dla systemów SCADA i ICS?   | 433 |
| Jakie są metody ochrony sieci przemysłowych przed atakami cybernetycznymi?   | 434 |

|   |     |
|---|-----|
| Co to jest standard IEC 62443 i jakie ma znaczenie dla bezpieczeństwa OT? | 435 |
| Jakie są kluczowe komponenty architektury Zero Trust?                     | 436 |
| Jaka jest różnica pomiędzy podatnością 0-day a 1-day?                     | 437 |
| Co oznacza skrót CTF?   | 437 |
| Co to są grupy APT i jakie stanowią zagrożenie?                           | 437 |
| Co to jest zasada czystego biurka, ekranu, druku i kosza?                 | 438 |
| Co to jest polityka retencji danych i dlaczego jest ważna?                | 439 |
| SŁOWO KOŃCOWE   | 440 |
| GDZIE SZUKAĆ DALEJ  | 443 |
| O AUTORZE   | 449 |
| O RECENZENTACH  | 450 |

# Kryptografia

## Co to jest kryptografia, jakie są jej główne cele i podstawowe zasady?

Kryptografia to dziedzina, która zajmuje się opracowywaniem metod zabezpieczania informacji przed nieuprawnionym dostępem, modyfikacją lub fałszowaniem. Polega na przekształcaniu danych (np. tekstu jawnego – *plaintext*) w formę nieczytelną (*ciphertext*) przy użyciu algorytmów i kluczy kryptograficznych. Poniżej przedstawiono jej główne cele oraz najważniejsze zasady:

| Cel  | Opis   |
|--|--|
| Poufność ( <i>Confidentiality</i> )          | Zapewnienie, że treść wiadomości pozostaje ukryta przed osobami niepowołanymi.     |
| Integralność ( <i>Integrity</i> )            | Gwarancja, że dane nie zostały zmienione w trakcie przesyłania lub przechowywania. |
| Autentykacja ( <i>Authentication</i> )       | Ustalenie tożsamości nadawcy i weryfikacja, czy jest on tym, za kogo się podaje.   |
| Niezaprzeczalność ( <i>Non-repudiation</i> ) | Uniemożliwienie wyparcia się autorstwa wysłanej lub podpisanej wiadomości.         |

Podstawowe zasady kryptografii:

- Zasada Kerckhoffsza – bezpieczeństwo systemu nie powinno zależeć od utajniania sposobu działania algorytmu, lecz od kluczy.
- Algorytmy symetryczne (*symmetric algorithms*) – ten sam klucz służy do szyfrowania i deszyfrowania danych; przykładami są *AES* czy *3DES*.
- Algorytmy asymetryczne (*asymmetric algorithms*) – wykorzystują klucz publiczny (*public key*, do szyfrowania) i klucz prywatny

(*private key*, do deszyfrowania lub podpisu cyfrowego); wśród popularnych algorytmów znajdują się *RSA* i *ECC*.

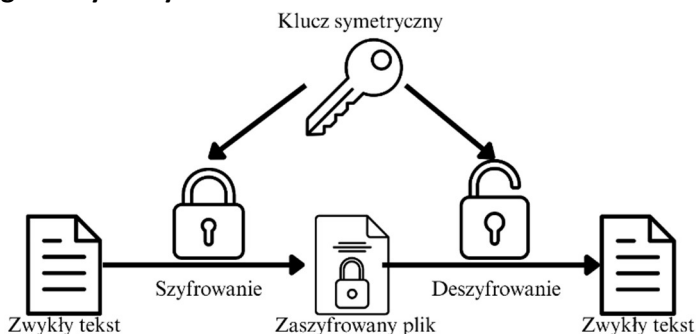
- Funkcje skrótu (*hash functions*) – przekształcają dowolny ciąg danych w ciąg o stałej długości, często wykorzystywane do weryfikacji integralności (np. *SHA-256*).
- Podpis cyfrowy (*digital signature*) – potwierdza autentyczność i integralność danych, opierając się zwykle na kryptografii asymetrycznej.

---

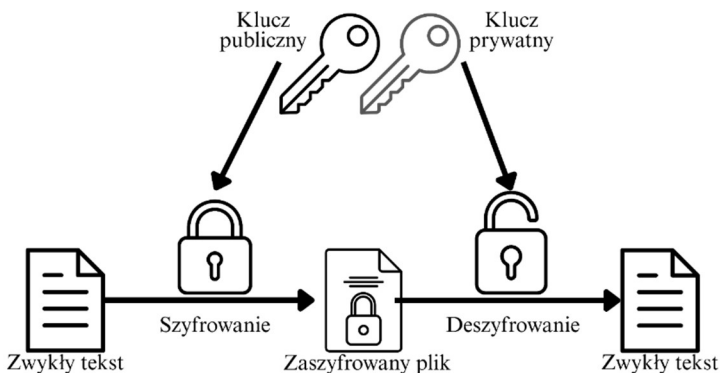
## Wyjaśnij różnicę między kryptografią symetryczną a asymetryczną i ich zastosowania.

**Kryptografia symetryczna** (*symmetric cryptography*) opiera się na jednym kluczu służącym zarówno do szyfrowania (*encryption*), jak i odszyfrowywania (*decryption*) danych. Z kolei **kryptografia asymetryczna** (*asymmetric cryptography*) wykorzystuje parę kluczy: publiczny (*public key*) i prywatny (*private key*). Różnice widać nie tylko w mechanice działania, ale też w typowych zastosowaniach obydwu metod.

### Kryptografia symetryczna



### Kryptografia asymetryczna



Porównanie kryptografii symetrycznej i asymetrycznej:

| Cecha                 | Kryptografia symetryczna ( <i>Symmetric Cryptography</i> ) | Kryptografia asymetryczna ( <i>Asymmetric Cryptography</i> ) |
|-----------------------|--|--|
| Liczba kluczy         | Jeden klucz (wspólny)                                      | Dwa klucze: publiczny i prywatny                             |
| Szybkość działania    | Zazwyczaj bardzo szybka                                    | Wolniejsza   |
| Skalowalność          | Problem rośnie przy większej liczbie użytkowników          | Łatwiejsza obsługa wielu użytkowników                        |
| Bezpieczeństwo kluczy | Klucz musi być przekazany w bezpieczny sposób              | Klucz publiczny można udostępniać otwarcie                   |
| Typowe zastosowania   | Szyfrowanie dysków, transmisja dużych plików, VPN          | Bezpieczna wymiana kluczy, podpisy cyfrowe                   |

Zastosowania w praktyce:

- Kryptografia symetryczna (np. *AES*):
  - Szyfrowanie dużych ilości danych (ze względu na szybkość).
  - Zabezpieczanie połączeń *VPN* i protokołów takich jak *IPSec*.
- Kryptografia asymetryczna (np. *RSA*, *ECC*):

- Bezpieczna dystrybucja kluczy do późniejszego użycia w algorytmach symetrycznych.
- Podpisy cyfrowe (*digital signatures*) służące weryfikacji tożsamości i integralności danych.
- Infrastruktura Klucza Publicznego (*Public Key Infrastructure, PKI*), np. w certyfikatach *SSL/TLS*.

Zwykle w praktycznych rozwiązaniach te dwa rodzaje kryptografii się łączą: asymetryczna jest wykorzystywana do wymiany klucza symetrycznego, a następnie do właściwego szyfrowania danych używa się algorytmu symetrycznego. Taka hybrydowa metoda (*hybrid method*) łączy zalety obu podejść: wygodę bezpiecznego rozpowszechniania kluczy i wysoką wydajność szyfrowania.

---

## Co to jest klucz kryptograficzny, jakie są jego rodzaje i jak zarządzać kluczami?

**Klucz kryptograficzny** (*cryptographic key*) to sekwencja bitów używana do szyfrowania (*encryption*) i deszyfrowania (*decryption*) danych lub do weryfikacji integralności (*integrity*) i autentyczności (*authenticity*) informacji. Klucze pełnią centralną rolę w systemach kryptograficznych, ponieważ bezpieczne przechowywanie i zarządzanie kluczami jest niezbędne do zachowania poufności (*confidentiality*) i wiarygodności danych.

### Rodzaje kluczy kryptograficznych:

| Rodzaj klucza                      | Opis  | Zastosowanie  |
|------------------------------------|---|---|
| Symetryczny ( <i>Symmetric</i> )   | Wykorzystuje jeden klucz do szyfrowania i deszyfrowania. Klucz musi być utrzymywany w tajemnicy przez wszystkie strony komunikacji. | Szyfrowanie dużych zbiorów danych (np. szyfrowanie dysków, transmisji VPN). Wysoka wydajność, ale trudniejsza dystrybucja kluczy. |
| Asymetryczny ( <i>Asymmetric</i> ) | Wykorzystuje parę kluczy: publiczny ( <i>public key</i> , ujawniany) i prywatny   | Szyfrowanie w komunikacji (np. <i>TLS</i> ), podpisy cyfrowe ( <i>digital</i> )   |

| Rodzaj klucza                         | Opis   | Zastosowanie  |
|---------------------------------------|--|---|
|                                       | ( <i>private key</i> , trzymany w tajemnicy).                          | <i>signatures</i> ), wymiana kluczy dla szyfrów symetrycznych. Wolniejszy, lecz prostszy w dystrybucji.   |
| Sesyjny ( <i>Session key</i> )        | Tworzony na krótki czas w trakcie konkretnego połączenia lub operacji. | Używany do jednorazowej, bezpiecznej komunikacji, np. w protokołach szyfrujących połączenie na czas sesji ( <i>SSL/TLS</i> ).                             |
| Ephemeryczny ( <i>Ephemeral key</i> ) | Generowany losowo i używany tylko raz albo bardzo krótko.              | Zwiększa poufność w protokołach (np. <i>Perfect Forward Secrecy</i> w <i>TLS</i> ), ograniczając ryzyko przechwycenia i odtworzenia klucza w przyszłości. |

### Zarządzanie kluczami (*Key Management*):

Poprawne zarządzanie kluczami to podstawa bezpieczeństwa kryptograficznego. Nawet najsilniejszy algorytm nie zagwarantuje ochrony, jeśli klucze nie będą przechowywane i dystrybuowane we właściwy sposób. Na zarządzanie kluczami składa się:

- Generowanie kluczy (*Key Generation*):
  - Wymaga wiarygodnego źródła losowości (np. generator liczb losowych spełniający normy *FIPS*).
  - Klucze powinny mieć odpowiednią długość zależną od algorytmu (np. *AES-256*, *RSA-2048/4096*).
- Dystrybucja i przechowywanie (*Distribution and Storage*):
  - Bezpieczne kanały komunikacji (np. protokoły szyfrujące, fizyczny transport w postaci tokenu).
  - Odpowiednie zabezpieczenia w oprogramowaniu i/lub sprzęcie (*HSM – Hardware Security Module*).

- Rotacja kluczy (*Key Rotation*):
  - Regularne zmiany kluczy ograniczają ryzyko związane z ich potencjalnym wyciekiem.
  - Dobrą praktyką jest ustalenie polityk okresowego odnawiania kluczy (np. co 90 lub 180 dni).
- Kontrola dostępu i audyt (*Access Control and Audit*):
  - Uprawnienia do używania, odczytu i modyfikacji kluczy muszą być ściśle ograniczone.
  - Monitorowanie i rejestrowanie użycia kluczy ułatwia wykrywanie nadużyć.
- Unieważnianie i niszczenie kluczy (*Key Revocation and Destruction*):
  - Jeśli klucz zostanie skompromitowany lub wygaśnie, należy go unieważnić (*revoke*).
  - Fizyczne usuwanie (np. wymazanie z pamięci) i zastąpienie nowym kluczem w celu uniemożliwienia odzyskania.

---

## Jak działa algorytm AES, czym jest szyfrowanie blokowe (*block cipher*) i jakie są tryby jego pracy (*ECB, CBC* itp.)?

**AES** (*Advanced Encryption Standard*) to symetryczny algorytm szyfrujący, uznawany za standard w obszarze kryptografii. Operuje na blokach danych o stałym rozmiarze 128 bitów i wykorzystuje klucze o długościach 128, 192 lub 256 bitów. Szyfrowanie blokowe (*block cipher*) oznacza, że dane są dzielone na bloki o ściśle określonym rozmiarze i każdy z nich jest przetwarzany niezależnie (choć w zależności od wybranego trybu pracy może istnieć powiązanie między blokami).

W dużym uproszczeniu *AES* przeprowadza serię rund szyfrujących, w których dane wejściowe (blok 128-bitowy) są poddawane operacjom takim jak:

- *SubBytes* – zastosowanie nietrwalej funkcji *S-Box* (zamiana bajtów na inne bajty),
- *ShiftRows* – przesunięcie wierszy w stanie (wewnętrznej reprezentacji bloku),
- *MixColumns* – mieszanie kolumn (z wyjątkiem ostatniej rundy),
- *AddRoundKey* – dodanie (bitowe *XOR*) podklucza wygenerowanego z klucza głównego.

Każdy z powyższych kroków utrudnia odzyskanie pierwotnych danych bez znajomości klucza. W zależności od rozmiaru klucza wykonuje się 10, 12 lub 14 rund.

### Tryby pracy AES (AES Modes of Operation)

Choć *AES* operuje na blokach 128-bitowych, w praktyce chcemy szyfrować dowolne ilości danych, często o wielkości większej niż jeden blok. Do tego służą tryby pracy (*modes of operation*). Oto najpopularniejsze:

| Tryb                               | Opis   | Zalety i wady   |
|------------------------------------|--|---|
| <i>ECB (Electronic Codebook)</i>   | Najprostszy tryb: każdy blok jest szyfrowany niezależnie, bez dodatkowego łączenia bloków.   | + Bardzo prosty w implementacji<br>- Bloki o tej samej treści szyfrują się tak samo, ujawniając wzory w danych  |
| <i>CBC (Cipher Block Chaining)</i> | Każdy blok przed szyfrowaniem jest łączony ( <i>XOR</i> ) z poprzednim zaszyfrowanym blokiem. Pierwszy blok łączy się z wektorem początkowym ( <i>Initialization Vector, IV</i> ). | + Ukrywa powtarzające się wzory w danych<br>- Wymaga niezmienności kolejności bloków; błędy propagują się dalej |
| <i>CFB (Cipher Feedback)</i>       | Realizuje szyfrowanie strumieniowe ( <i>stream cipher</i> ) na bazie szyfru blokowego, wykorzystuje  | + Może szyfrować dane w mniejszych porcjach niż rozmiar bloku<br>- Może wolniej działać w                       |

# O Autorze

**Wojciech Ciemski** to specjalista cyberbezpieczeństwa z ponad dziesięcioletnim doświadczeniem w branży IT, koncentrujący się na defensywnych aspektach ochrony informacji. Jego obszary pracy obejmują bezpieczeństwo operacyjne, threat intelligence, audyty bezpieczeństwa oraz testy penetracyjne.

Jest założycielem bloga Security Bez Tabu®, który stanowi jedno z najbardziej rozpoznawalnych źródeł wiedzy o cyberbezpieczeństwie w Polsce. Publikuje tam materiały oparte na praktyce – analizy scenariuszy ataków, podejścia do detekcji zagrożeń oraz konkretne rozwiązania problemów, z którymi mierzą się zespoły bezpieczeństwa.

W 2024 roku znalazł się na globalnej liście „40 under 40 in Cybersecurity” jako jedyny reprezentant Polski. Od 2021 roku regularnie występuje na konferencjach branżowych, gdzie porusza tematy związane z praktycznym zastosowaniem cyberbezpieczeństwa w organizacjach.

Jest autorem serii „Cybersecurity w pytaniach i odpowiedziach”, skierowanej zarówno do osób rozpoczynających pracę w branży, jak i specjalistów porządkujących swoją wiedzę. Tworzy również programy szkoleniowe oparte na scenariuszach rzeczywistych, w tym „30-dniowe Wyzwanie Security”, w których uczestnicy pracują na zadaniach odzwierciedlających codzienną pracę w cyberbezpieczeństwie.

W swojej działalności edukacyjnej stawia na bezpośredni, techniczny przekaz oraz nacisk na praktykę. W ostatnich latach przeprowadził setki godzin szkoleń, pracując z osobami na różnych etapach kariery – od początkujących po specjalistów.

Traktuje cyberbezpieczeństwo jako proces wymagający ciągłego rozwoju, krytycznego myślenia i świadomego podejścia do ryzyka. Jego celem jest przekazywanie wiedzy w sposób użyteczny – taki, który można realnie zastosować w pracy.

# O recenzentach

**Esmeralda Kazia** pełni funkcję Dyrektora ds. Monitorowania i Reagowania na Incydenty w Centrum Operacyjnym SOC C-SIRT przy Narodowym Urzędzie ds. Cyberbezpieczeństwa (NCSA) w Albanii. Odpowiada za nadzór nad krajowymi operacjami bezpieczeństwa, w tym wykrywanie, analizę i reagowanie na incydenty w czasie rzeczywistym.

W 2025 roku została wyróżniona na liście „40 Under 40 in Cybersecurity”, obejmującej liderów młodego pokolenia w tej dziedzinie. Reprezentowała Albanię m.in. podczas paneli Komitetu Bezpieczeństwa OBWE w Wiedniu, gdzie omawiała rozwój zagrożeń oraz budowanie odporności cyfrowej na poziomie państwowym.

Angażuje się również w inicjatywy wspierające rozwój kompetencji w sektorze cyberbezpieczeństwa, w tym działania na rzecz zwiększenia udziału kobiet w branży IT. Regularnie występuje publicznie i publikuje materiały dotyczące bezpieczeństwa infrastruktury krytycznej, ochrony danych oraz zagrożeń związanych z rozwojem sztucznej inteligencji.

**Kunal Sehgal** posiada ponad 19 lat doświadczenia w obszarze cyberbezpieczeństwa, w tym na stanowiskach kierowniczych w sektorze finansowym. Specjalizuje się w budowie i zarządzaniu usługami bezpieczeństwa oraz rozwijaniu programów cyberbezpieczeństwa w skali regionalnej.

Odegrał istotną rolę w tworzeniu dwóch organizacji typu ISAC (Information Sharing and Analysis Centers) w Singapurze, wspierających wymianę informacji o zagrożeniach w regionie Azji i Pacyfiku. Współpracował z krajowymi zespołami CERT, regulatorami oraz instytucjami rządowymi w zakresie przeciwdziałania cyberzagrożeniom.

Jego doświadczenie obejmuje zarówno aspekty techniczne, jak i zarządcze – od projektowania architektury bezpieczeństwa po wdrażanie mechanizmów nadzoru i zarządzania ryzykiem. Jest autorem publikacji branżowych, prowadzi działalność edukacyjną oraz posiada liczne certyfikaty i kwalifikacje zawodowe związane z cyberbezpieczeństwem.