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

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

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

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

Podstawowe zasady kryptografii:

- Zasada Kerckhoffsa – 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*.

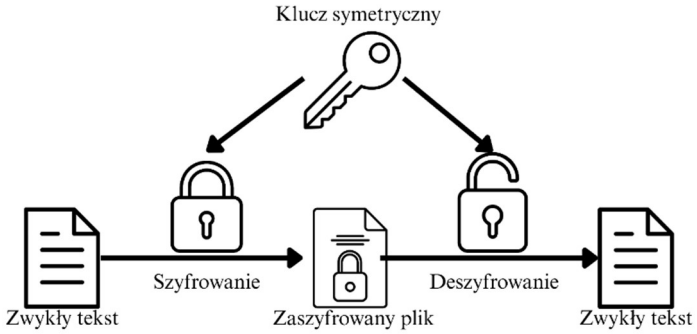
- Funkcje skrótu (*hash functions*) – przekształcają dowolny ciąg danych w ciąg o stałej długości, często wykorzystywane do weryfikacji integralności (np. *SHA-256*).

- Podpis cyfrowy (*digital signature*) – potwierdza autentyczność i integralność danych, opierając się zwykle na kryptografii asymetrycznej.

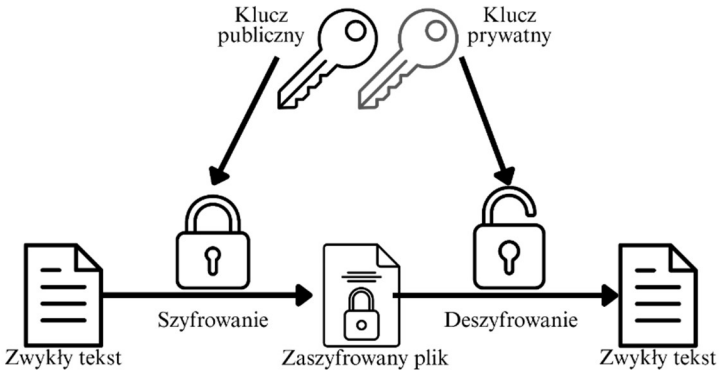
Wyjaśnij różnicę między kryptografią symetryczną a asymetryczną i ich zastosowania.

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 (*Symmetric Cryptography*)**	**Kryptografia asymetryczna (*Asymmetric Cryptography*)**
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 łączy: 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 (*Symmetric*)	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 (*Asymmetric*)	Wykorzystuje parę kluczy: publiczny (*public key*, ujawniany) i prywatny	Szyfrowanie w komunikacji (np. *TLS*), podpisy cyfrowe (*digital*

Rodzaj klucza	Opis	Zastosowanie
	(*private key*, trzymany w tajemnicy).	*signatures*), wymiana kluczy dla szyfrów symetrycznych. Wolniejszy, lecz prostszy w dystrybucji.
Sesyjny (*Session key*)	Tworzony na krótki czas w trakcie konkretnego połączenia lub operacji.	Używany do jednorazowej, bezpiecznej komunikacji, np. w protokołach szyfrujących połączenie na czas sesji (*SSL/TLS*).
Ephemeryczny (*Ephemeral key*)	Generowany losowo i używany tylko raz albo bardzo krótko.	Zwiększa poufność w protokołach (np. *Perfect Forward Secrecy* w *TLS*), 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 nietrwałej 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**
ECB (*Electronic Codebook*)	Najprostszy tryb: każdy blok jest szyfrowany niezależnie, bez dodatkowego łączenia bloków.	+ Bardzo prosty w implementacji - Bloki o tej samej treści szyfrują się tak samo, ujawniając wzory w danych
CBC (*Cipher Block Chaining*)	Każdy blok przed szyfrowaniem jest łączony (*XOR*) z poprzednim zaszyfrowanym blokiem. Pierwszy blok łączy się z wektorem początkowym (*Initialization Vector*, *IV*).	+ Ukrywa powtarzające się wzory w danych - Wymaga niezmienności kolejności bloków; błędy propagują się dalej
CFB (*Cipher Feedback*)	Realizuje szyfrowanie strumieniowe (*stream cipher*) na bazie szyfru blokowego, wykorzystuje	+ Może szyfrować dane w mniejszych porcjach niż rozmiar bloku - 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.