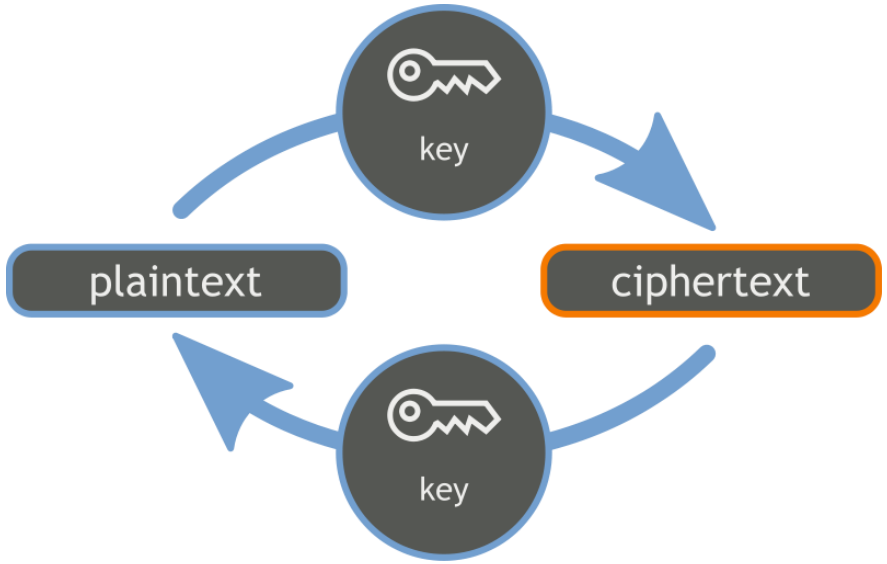
Kwantowe algorytmy kryptograficzne

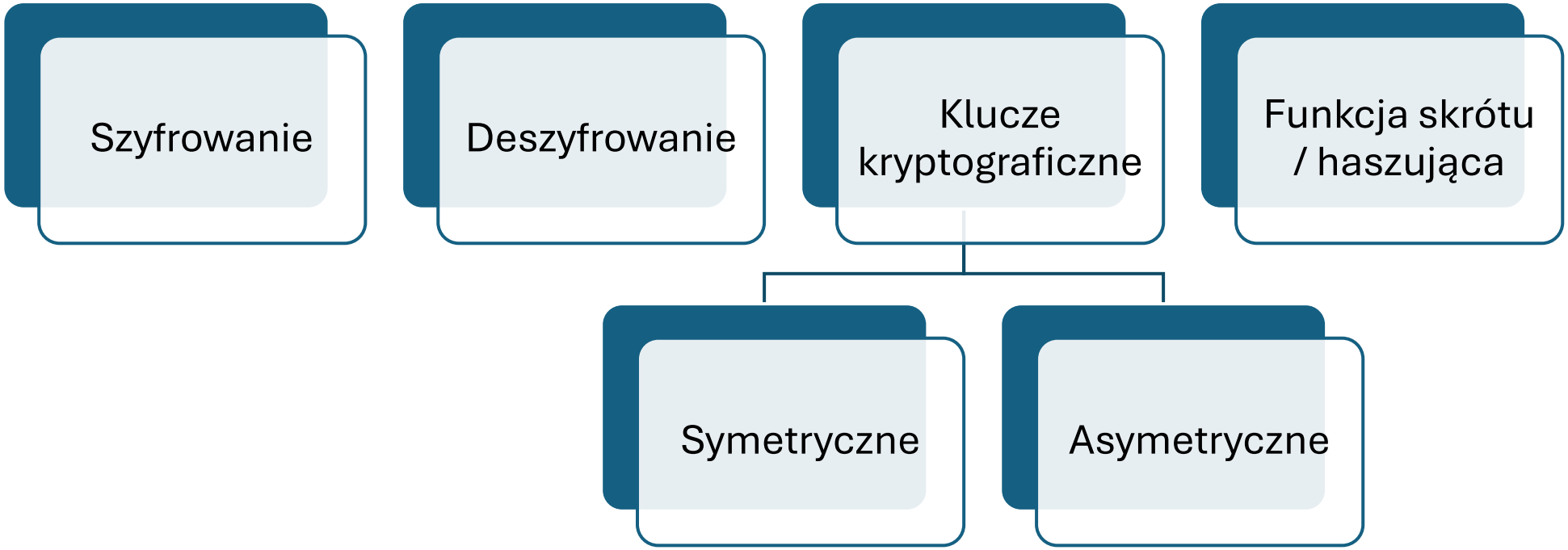
145259

Czym jest kryptografia?

Kryptografia to dziedzina nauki i technologii zajmująca się zabezpieczaniem informacji przed nieautoryzowanym dostępem, zapewnieniem ich poufności, integralności, autentyczności oraz nierozłączności.



Najważniejsze elementy kryptografii



Cele kryptografii

- Poufność
- Integralność
- Autentyczność
- Nierozłączność

Algorytmy kryptograficzne

Algorytmy kryptograficzne – metody służące zabezpieczeniu informacji przed odczytem przez nieupoważnione osoby. Odbywa się to poprzez przekształcenie w informacji w sposób znany tylko dla właściwych osób.

PQC

Q-DAY

- Post-quantum cryptography (PQC) – czyli po polsku kryptografia postkwantowa – jest to nauka zajmująca się algorytmami kryptograficznymi, które mają być odporne na złamanie za pomocą komputera kwantowego.

Kwantowe algorytmy kryptograficzne

- Kryptologia kwantowa – metody wykonywania zadań kryptograficznych przy użyciu informatyki kwantowej.
- Wykorzystują zasady mechaniki kwantowej do tworzenia i łamania zabezpieczeń.
- Dane przechowywane są w kubitach, a nie w bitach.

Algorytm Shora

Algorytm faktoryzacji Shora – algorytm kwantowy umożliwiający rozkład na czynniki pierwsze liczby naturalnej N przy wykorzystaniu komputera kwantowego.

RSA – asymetryczny algorytm kryptograficzny z kluczem publicznym. Bezpieczeństwo szyfrowania polega na trudności faktoryzacji dużych liczb złożonych. Długość: 1024, 2048, 3072, 4096.

Algorytm Shora

- Jest to algorytm kwantowy, co oznacza, że jak większość innych algorytmów zwraca wynik obarczony pewnym prawdopodobieństwem.
- Na wejściu algorytmu dostajemy liczbę naturalną N. Naszym zadaniem jest znalezienie liczby p między 1 a N, która dzieli N bez reszty.
- Składa się z dwóch części:
  - Komputer klasyczny – sprowadzenie problemu faktoryzacji do problemu znajdowania rzędu elementu w grupie
  - Komputer kwantowy – znajdowania rzędu elementu

Algorytm Grovera

- Przyspiesza wyszukiwania w niestrukturalnych bazach danych.
- Może służyć do atakowania symetrycznych algorytmów szyfrujących, takich jak AES

Inne algorytmy

- Kwantowa dystrybucja klucza (QKD)
- Kwantowy podpis cyfrowy
- Kwantowe homomorficzne szyfrowanie
- Protokół kryptograficzny Wiesnera (Quantum Money)

Kryptografia klasyczna a kwantowa

Klasyczna	Kwantowa
Działanie	
Trudność matematycznych problemów	Zasady mechaniki kwantowej
Bezpieczeństwo	
Możliwość ich złamania poprzez zaawansowane algorytmy kwantowe	Gwarantują bezpieczeństwo, umożliwiają wykrywalność podsłuchu i manipulacji
Stan na dzisiaj	
Algorytmy kryptografii klasycznej są dobrze poznane i szeroko stosowane	Algorytmy kryptografii kwantowej są nadal w fazie rozwoju oraz testów, są stosowane tylko w niektórych, zaawansowanych, systemach bezpieczeństwa

Dziękuję za uwagę

Literatura

- https://utimaco.com/service/knowledge-base/post-quantum-cryptography/what-shors-algorithm
- https://www.classiq.io/insights/shors-algorithm-explained
- https://en.wikipedia.org/wiki/Shor%27s_algorithm
- https://learning.quantum.ibm.com/course/fundamentals-of-quantum-algorithms/grovers-algorithm