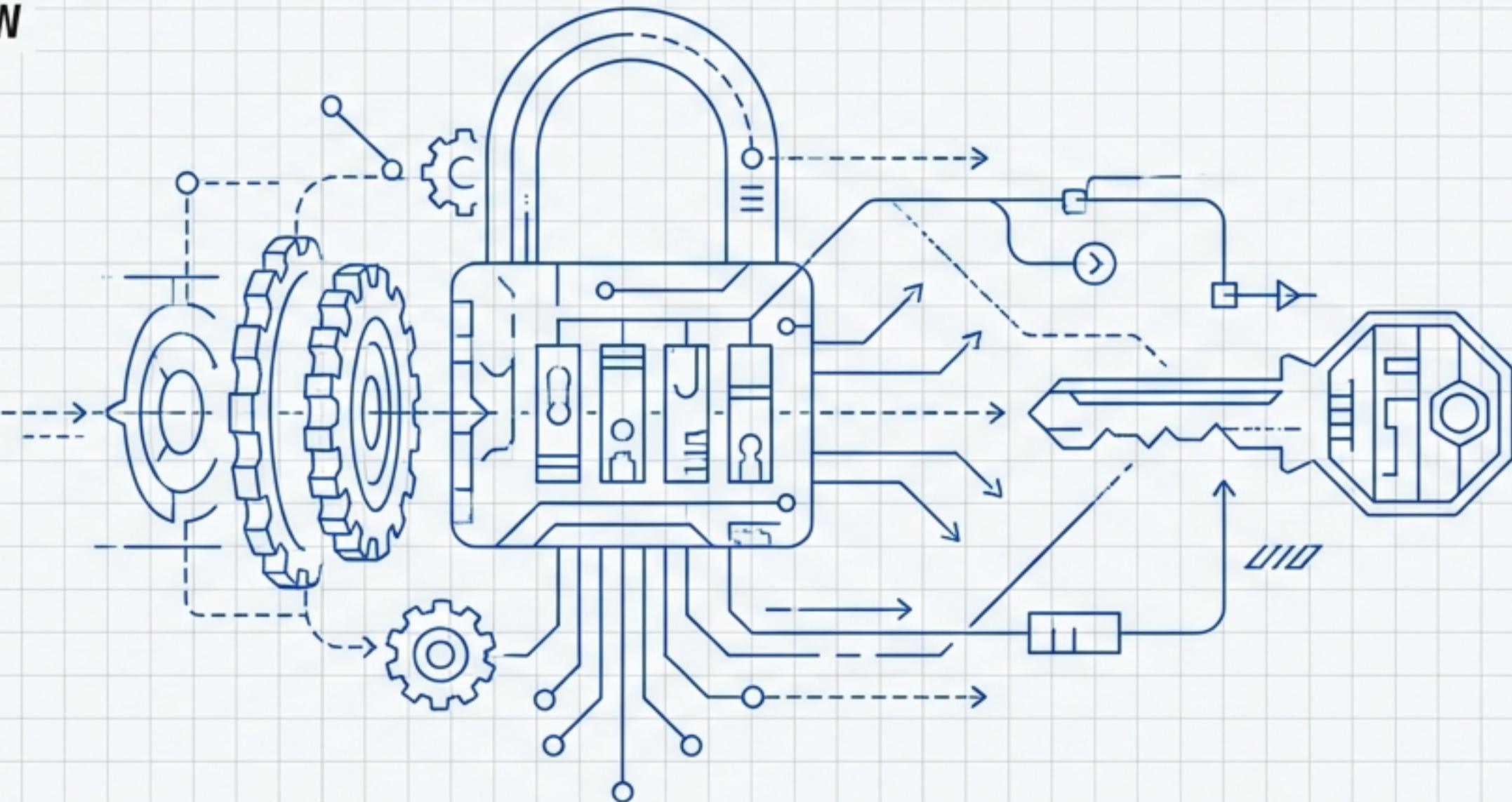


KRYPTOGRAFIA: PROJEKT PRAKTYCZNY

Implementacja mechanizmów
bezpieczeństwa danych



CEL OPERACYJNY

Głównym celem projektu jest zdobycie praktycznych kompetencji w zakresie zabezpieczania informacji cyfrowych. Projekt skupia się na technicznej implementacji standardów bezpieczeństwa.

- Poznanie mechanizmów szyfrowania danych
- Implementacja podpisów cyfrowych
- Praktyczne zastosowanie narzędzi Open Source



ARSENAŁ NARZĘDZI

GPG

(GNU Privacy Guard)



Implementacja standardu OpenPGP do szyfrowania i podpisywania danych.

OpenSSL

(Secure Sockets Layer Toolkit)



Biblioteka kryptograficzna zapewniająca bezpieczną komunikację w sieci.

INICJALIZACJA ŚRODOWISKA

Konfiguracja systemu

```
$ sudo apt update  
$ sudo apt install -y gnupg openssl
```



Instalacja pakietów niezbędnych do realizacji zadań.

WERYFIKACJA ZASOBÓW

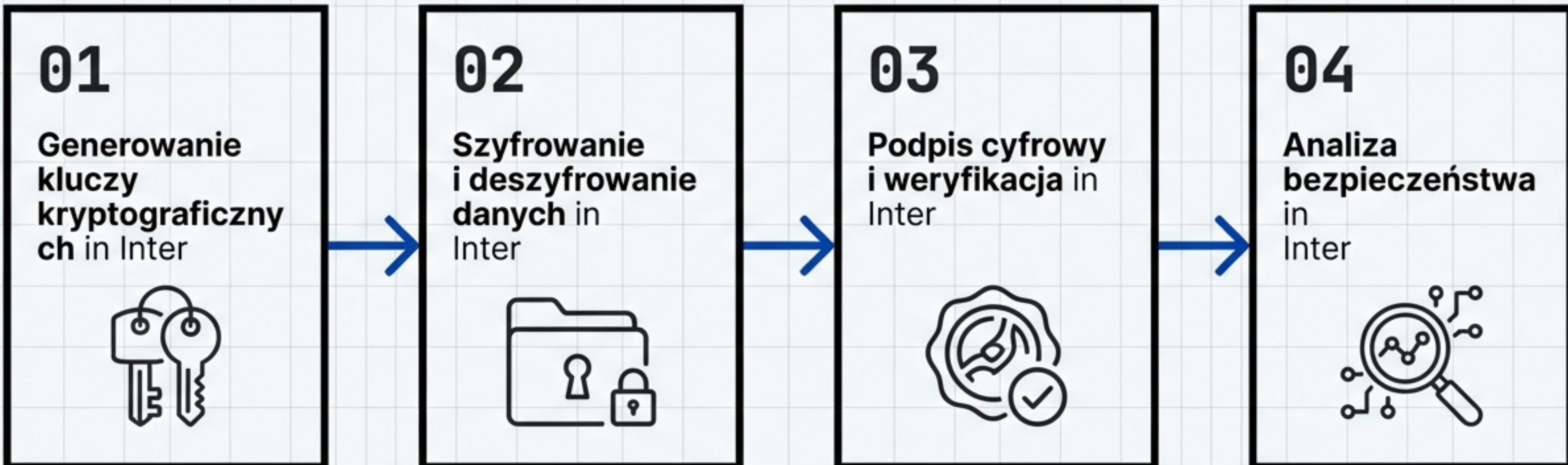
Kontrola wersji

```
$ gpg --version  
$ openssl version
```

Status: Wymagane sprawdzenie poprawności instalacji.

Cel: Potwierdzenie gotowości operacyjnej narzędzi.

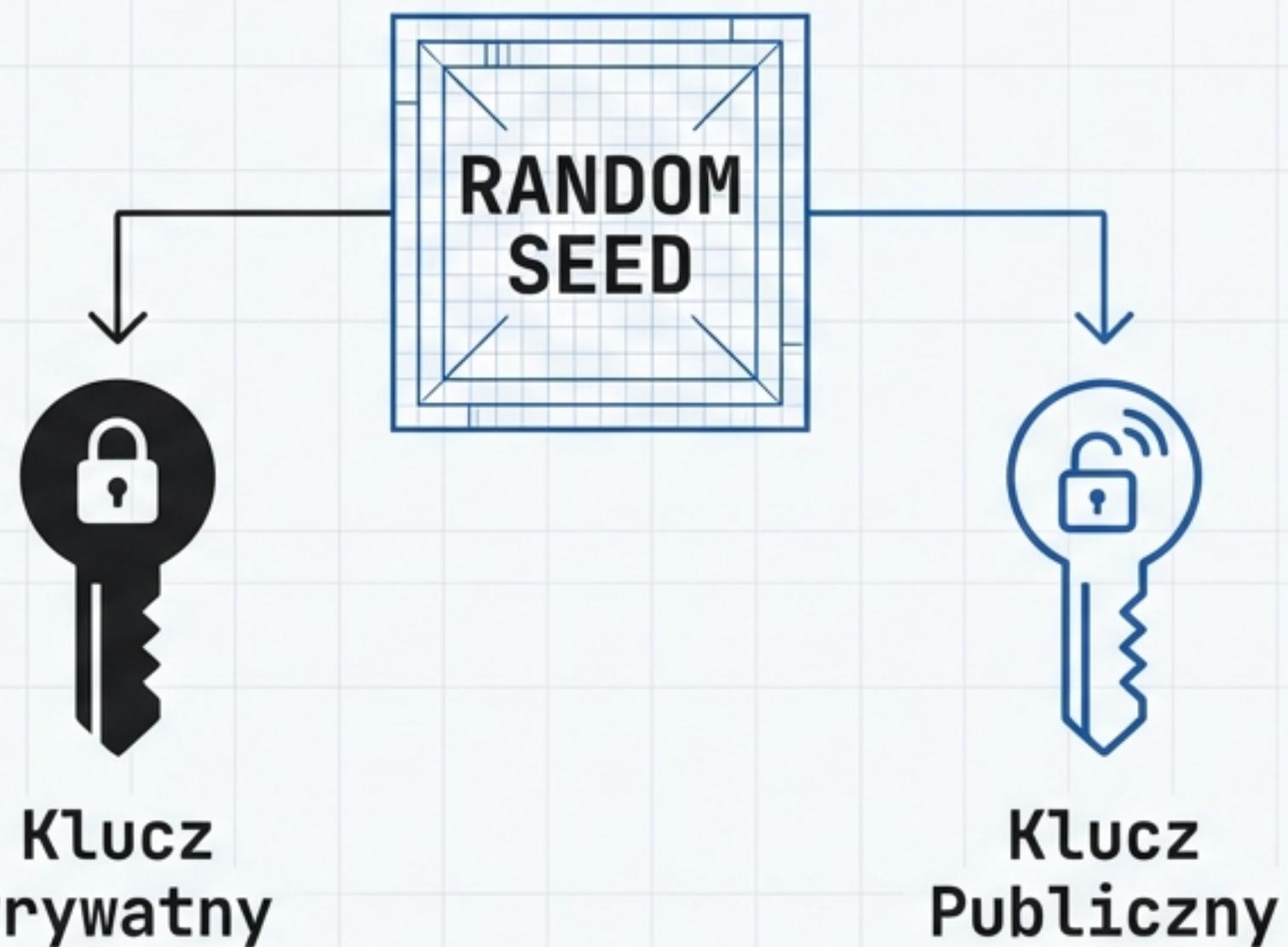
ZAKRES DZIAŁAŃ



FAZA 1: GENEROWANIE KLUCZY

Podstawa bezpiecznej komunikacji.

Proces ten obejmuje tworzenie unikalnych par kluczy (prywatny i publiczny), które stanowią fundament tożsamości w systemie kryptograficznym.

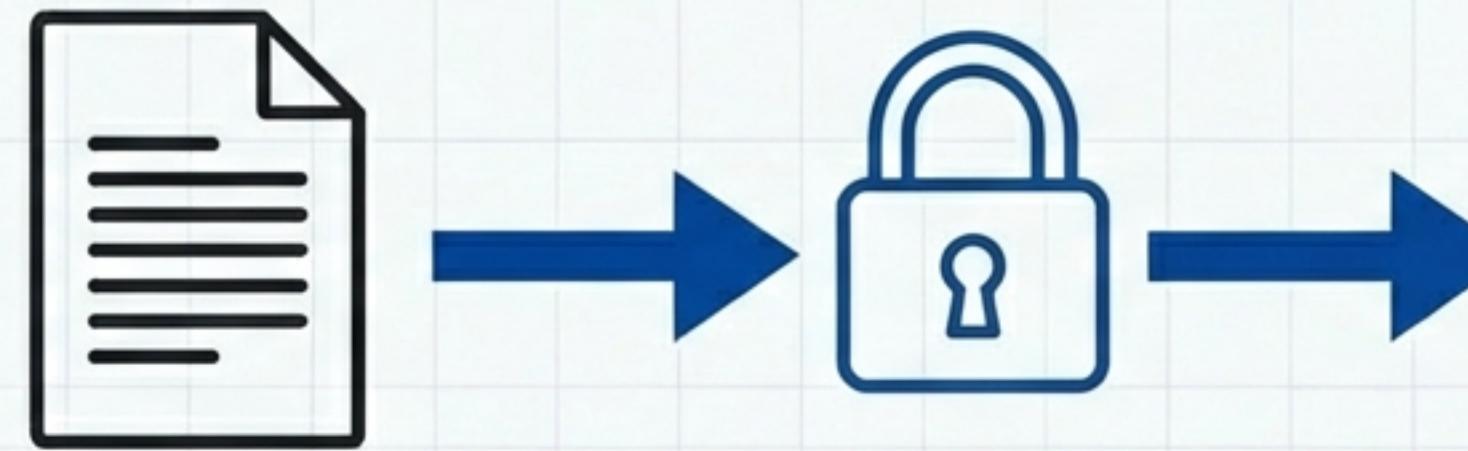


FAZA 2: SZYFROWANIE DANYCH

Poufność informacji.

Wykorzystanie algorytmów do przekształcania tekstu jawnego w szyfrogram.

Dostęp do treści możliwy jest tylko dla posiadacza odpowiedniego klucza.



Tekst Jawny

Szyfrowanie

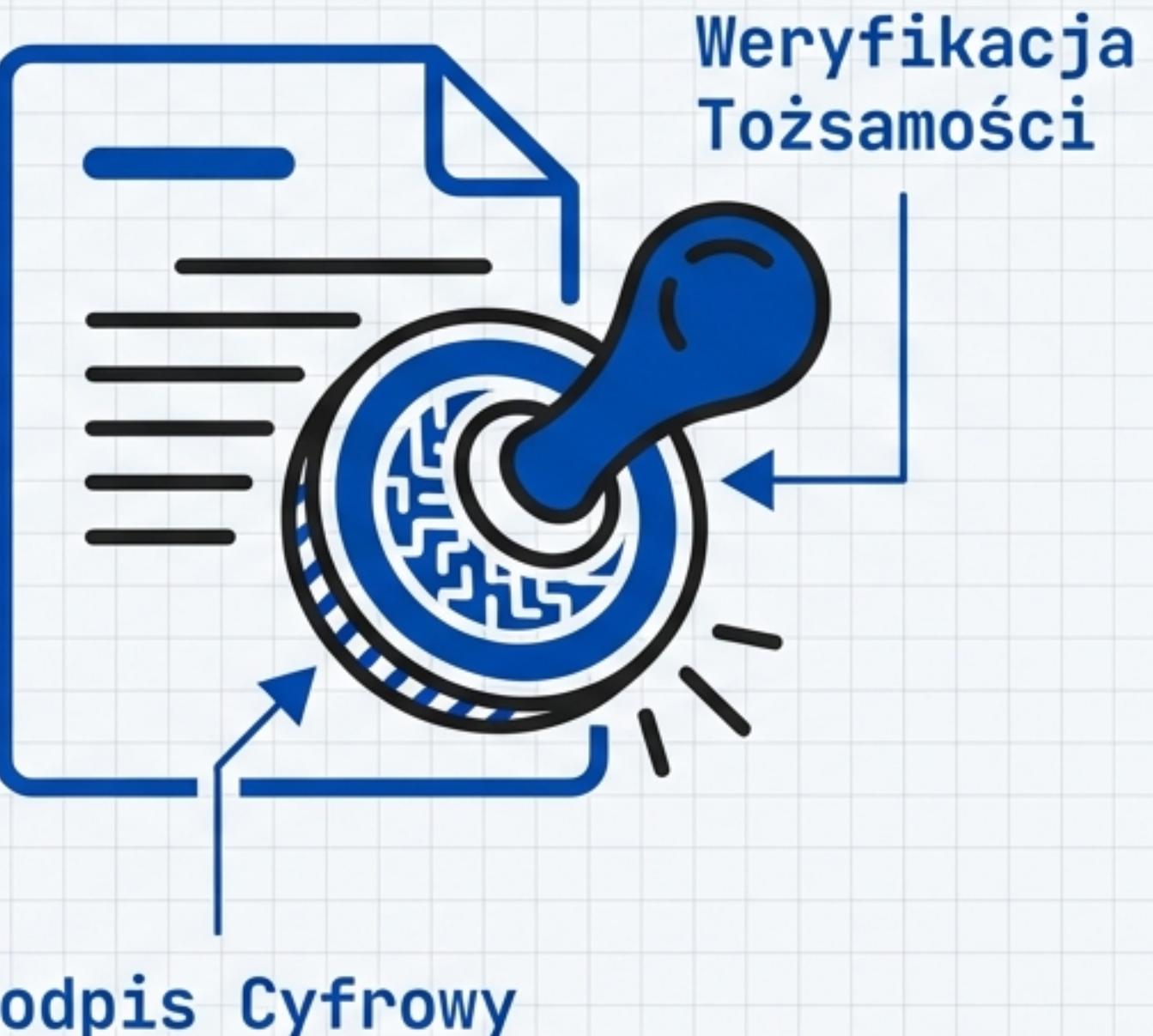
10011010
01100101
11011001
10101010
0>/#\$+]@

Szyfrogram

FAZA 3: UWIERZYTELNIANIE

Integralność i tożsamość.

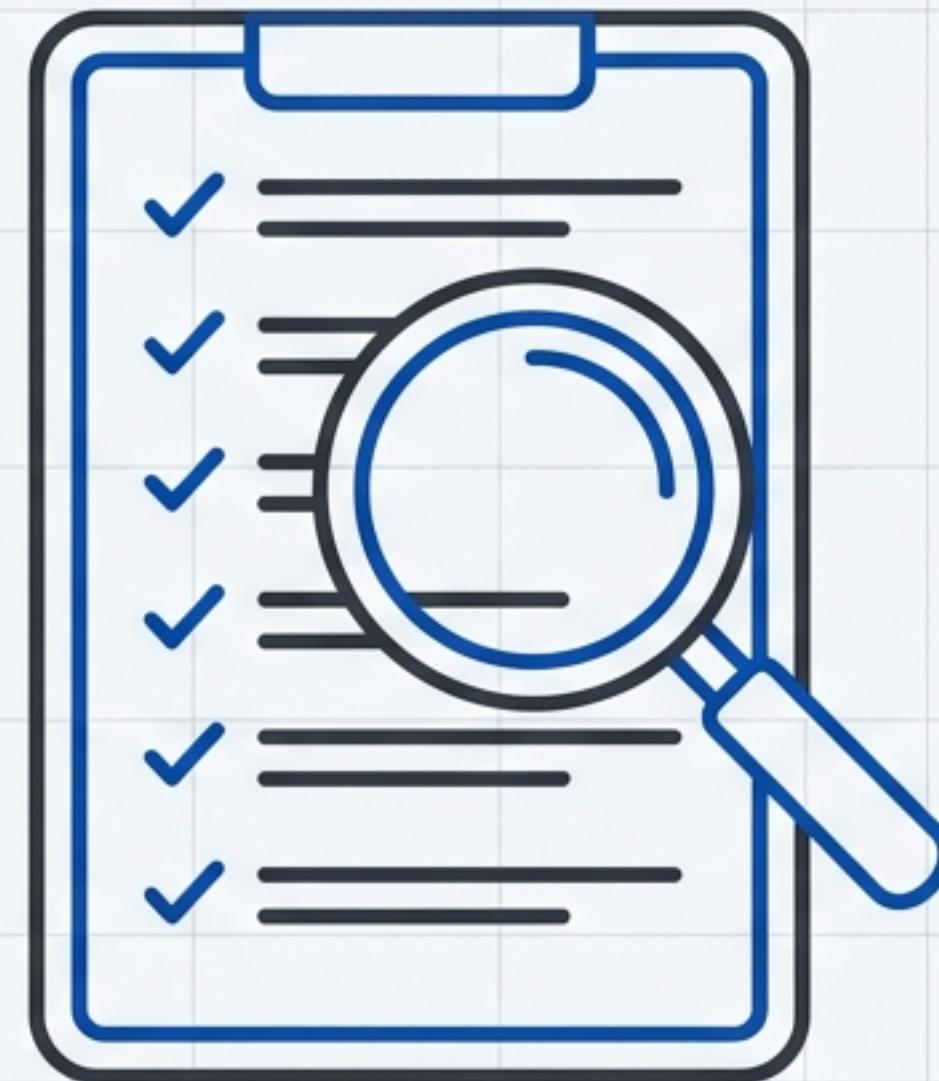
Zastosowanie podpisu cyfrowego gwarantuje, że wiadomość pochodzi od zaufanego nadawcy i nie została zmodyfikowana w trakcie transmisji.



FAZA 4: AUDYT

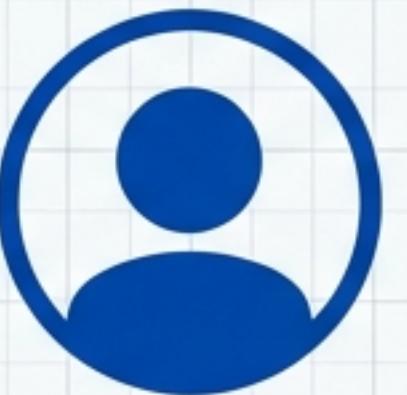
Analiza bezpieczeństwa.

Krytyczny przegląd zaimplementowanych rozwiązań pod kątem potencjalnych podatności oraz weryfikacja siły zastosowanych kluczy.

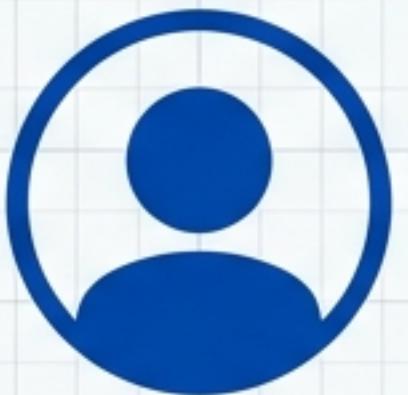


Raport Bezpieczeństwa

ZESPÓŁ REALIZACYJNY



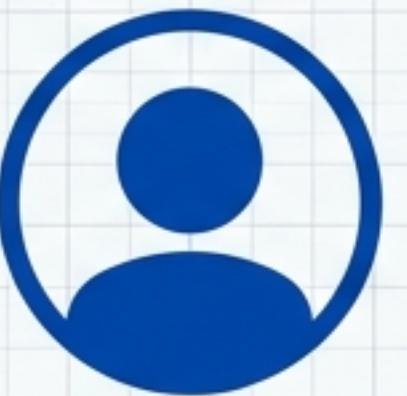
Marcel Maciejski



Szymon Goska



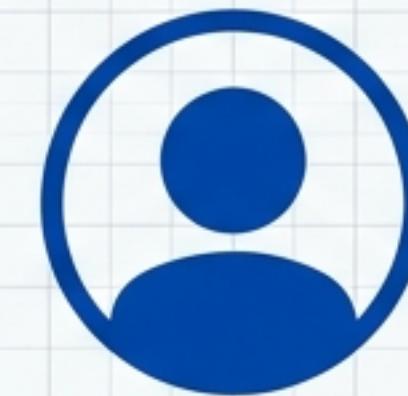
Dominik Olewiński



Adrian Paziewski



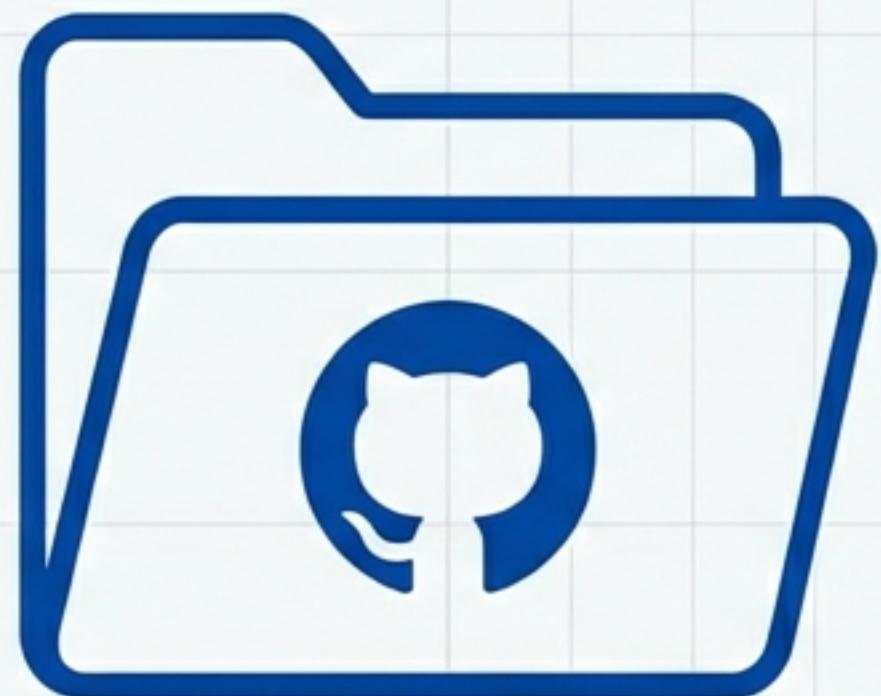
Daniel Pieńczykowski



Jan Rozenbajgier

DOKUMENTACJA ŹRÓDŁOWA

Pełny kod i opis implementacji dostępny w repozytorium.



github.com/Mmaciejski/Projekt-Kryptografia