WYŻSZA SZKOŁA HANDLOWA W RADOMIU


RADOM ACADEMY OF ECONOMICS

# Wyższa Szkoła Handlowa w Radomiu

# Podstawy kryptografii
# Laboratorium 3

**Radom 2020/2021**

# 1. Cel zadania

Zadanie polegać będzie na przeanalizowaniu działania najpopularniejszych technik szyfrowania dokumentów.

# 2. Potrzebne narzędzia.

- system Windows co najmniej w wersji 8.1, 32-bitowy (lub nowszy, 64-bitowy)
- program CryptTool (https://www.cryptool.org/en/ct1/downloads)

# 3. Informacje wstępne

W dzisiejszych czasach szyfrowanie oraz poświadczenie swojej tożsamości zaczyna odgrywać jedną z najważniejszych ról (o ile nie największą). Ludzie coraz bardziej przyzwyczajają się do wygody użytkowania zdobyczy nauki, takich jak płatności elektroniczne, przesyłanie danych do chmury obliczeniowej, dzielenie się danymi poufnymi z najbliższymi przy pomocy systemu rozproszonych danych itp. Przed projektantami tego typu rozwiązań stoi coraz większe wyzwanie, przy okazji coraz większa odpowiedzialność.

Na dzień dzisiejszy wykorzystuje się wiele dość popularnych rozwiązań, które są wystarczające by zapewnić zarówno poufność danych, jak i ich integralność. Warto zapoznać się z działaniem takich algorytmów jak symetryczne AES (wykorzystywane np. w sieciach bezprzewodowych), jak i asymetryczne RSA (wykorzystywane przy połączeniach SSH). Warto także zapoznać się z działaniem protokołów wymiany kluczy, powszechnie stosowanym np. w połączeniach tunelowych VPN.

# 4. Przebieg.

Po instalacji programu podanego w punkcie 2 należy go uruchomić. Dla laboratorium kluczowe będzie zapoznanie się z działaniem następujących metod szyfrowania:

- Cezar
- Zamiana
- Dodawanie bitów
- XOR
- DES z ECD
- DES z CBC
- AES
- RSA
- RSA z AES

Wspomniane szyfry należy przeanalizować co najmniej na dwóch szyfrowanych plikach/zestawie danych, wraz z dokonaniem odszyfrowania danych (celem sprawdzenia poprawności działania przykładu). Ponadto tam, gdzie program umożliwia analizę graficzną działania algorytmów, należy takową przeprowadzić.

# 5. Zakończenie

Z przebiegu laboratorium należy sporządzić sprawozdanie. W głównej mierze należy scharakteryzować każdy z testowanych algorytmów i wskazać jego wady oraz zalety. Sprawozdanie można oprzeć w głównej mierze na omówieniu zrzutów ekranu wykonanych podczas analizy wskazanych algorytmów szyfrujących. Sprawozdania mają mieć charaktery pracy indywidualnej (własne przykłady – proszę nie korzystać z domyślnego pliku tekstowego otwartego w programie).