**Wrocław 01.10.2024**

**Bezpieczeństwo i ochrona danych**

**Laboratorium nr 4**

**Asymetryczne algorytmy szyfrowania**

**Plan zajęć**

[I. Asymetryczne algorytmy szyfrowania.](#_Toc142226861)

[II. Zapoznanie się ze środowiskiem pracy - program CrypTool.](#_Toc142226862)

[III. Własności algorytmów asymetrycznych.](#_Toc142226863)

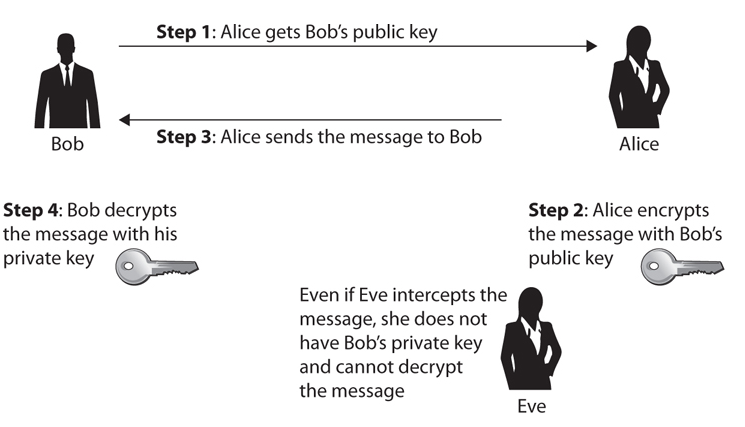
[IV. Raport z przeprowadzonych eksperymentów.](#_Toc142226864)

# Asymetryczne algorytmy szyfrowania.

Laboratorium przedstawia zagadnienia związane z szyfrowaniem asymetrycznym. Kryptografia z kluczem asymetrycznym opiera się na jednym kluczu do szyfrowania i innym, ale powiązanym kluczu do odszyfrowywania. Bardzo ważne jest, aby pamiętać, że nawet przy znajomości algorytmu kryptograficznego i klucza szyfrowania obliczeniowo niemożliwe jest określenie klucza deszyfrującego. Zaletą systemu jest to, że każda komunikująca się strona potrzebuje tylko pary kluczy do komunikacji z dowolną liczbą innych komunikujących się stron. Poza tym niektóre algorytmy, takie jak RSA, również wykazują ważną cechę, tj. jeden z dwóch powiązanych kluczy może być użyty do szyfrowania, a drugi do odszyfrowania.

Kryptografia asymetryczna opiera się na funkcjach jednokierunkowych - takich, które można łatwo obliczyć w jednym kierunku, ale bardzo trudno obliczyć w drugim. Istnieją dwa rodzaje algorytmów asymetrycznych. Pierwsza, nazywana „problemem faktoryzacji”, której bezpieczeństwo szyfrowania opiera się na trudności w rozłożeniu na czynniki iloczynu dwóch dużych liczb pierwszych. Na przykład mnożenie jest łatwe, a rozłożenie na czynniki (faktoryzacja) jest trudne (na czym RSA jest na przykład. Drugi typ to algorytmy oparte na kryptografii krzywych eliptycznych, których bezpieczeństwo opiera się na złożoności obliczeniowej dyskretnych logarytmów na krzywych eliptycznych - znane jako problem dyskretnego logarytmu krzywej eliptycznej (ECDLP). Wzmocnienie modulo jest łatwe , a dyskretne loga-rytmowanie jest trudne (dotyczy to takich algorytmów jak ElGamal, DSA i ECC).

Wbrew powszechnemu przekonaniu, Diffie-Hellman był pierwszym publicznie opisanym algorytmem asymetrycznym (nie RSA). Ten protokół kryptograficzny umożliwia dwóm podmiotom ustanowienie wspólnego klucza w niezabezpieczonym kanale. Innymi słowy, Diffie-Hellman jest często używany do umożliwienia aktorom wymiany klucza symetrycznego za pośrednictwem niezabezpieczonego medium, takiego jak Internet. Pomimo upływu czasu protokół DH jest nadal szeroko stosowany, na przykład w najnowszej wersji TLSv 1.3 (Transport Layer Security). ElGamal jest oparty na algorytmie wymiany kluczy Diffie-Hellman i jest używany w niektórych wersjach Pretty Good Privacy (PGP).



Rysunek 1 Wymiana wiadomości za pomocą kryptografii asymetrycznej

Opis kryptografii asymetrycznej z matematycznego punktu widzenia. Tekst jawny jest szyfrowany w blokach. Dla pewnych bloków tekstu jawnego M i bloku szyfrującego C, cały proces można podsumować następująco:

1. Wybieramy dwie duże liczby pierwsze  i  , takie, że .
2. Oblicz .
3. Oblicz .
4. Wybierz liczbę całkowitą  jako klucz publiczny (klucz szyfrujący) jednak nie może być współczynnikiem .
5. Oblicz jako klucz prywatny (klucz deszyfrujący) taki że:



1. Zakładając tekst jawny*,* szyfrogram należy obliczyć następująco:



1. Szyfrogram ten jest wysyłany do odbiorcy w celu odszyfrowania..
2. Szyfrogram jest odszyfrowywany w następujący sposób:



* Proszę zapoznać się z charakterystyką asymetrycznych algorytmów szyfrowania.
* Można również znaleźć odpowiednie opisy na stronach:

http://cacr.uwaterloo.ca/hac/about/chap8.pdf  
http://pl.wikipedia.org/wiki/Kryptografia\_asymetryczna<http://pl.wikipedia.org/wiki/RSA_(kryptografia>[)](http://www.ehaker.com/artykuly-wiecej/29/)<http://pl.wikipedia.org/wiki/ElGamal><http://pl.wikipedia.org/wiki/Digital_Signature_Algorithm><http://pl.wikipedia.org/wiki/Kryptografia_krzywych_eliptycznych>  
<http://en.wikipedia.org/wiki/Public-key_cryptography>

# Zapoznanie się ze środowiskiem pracy - program CrypTool.

* Na tych zajęciach laboratoryjnych będą wykorzystywane głównie narzędzia dostępne z zakładki z programu CrypTool:
  + *Szyfrowanie/Asymetryczne*
  + *Podpis cyfrowy/PKI/…*

# Własności algorytmów asymetrycznych.

**Zadania:**

### Proszę zapoznać się z demonstracją algorytmu RSA (*Szyfrowanie/Asymetryczne/Demonstracja RSA)*

### Proszę wygenerować następujące klucze kryptograficzne: ( *Podpis cyfrowy/PKI/Generowanie klucza/Import klucza)*

##### RSA długość 512 bitów,

##### RSA długość 1024 bitów,

##### RSA długość 2048 bitów,

### Dla trzech długości klucza (512,1024,2048) oraz dla trzech ustalonych tekstów jawnych (TJ) o różnych entropiach (np. tekst jednorodny, tekst średnio zróżnicowany, tekst bardzo zróżnicowany) należy porównać entropię TJ z entropią po zaszyfrowaniu (entropią tekstu tajnego TT). Proszę przyjrzeć się również autokorelacji TT i TJ.

### Dla różnych długości klucza algorytmu RSA zmierzyć czas szyfrowania i deszyfrowania plików o rozmiarze 1MB, 2MB, 5MB (dokładność do około sekudny).

### Pliki z punktu 4. zaszyfrować i odszyfrować algorytmem symetrycznym próbując zaobserwować czas realizacji tych operacji.

### Do kryptogramów utworzonych przy użyciu kluczy o różnej długości wprowadzić następujące zmiany:

##### zmienić wartość 1 bajtu,

##### usunąć 1 bajt,

##### usunąć kilka (kilkadziesiąt) bajtów,

##### usunąć fragment równy długości modułu algorytmu (512,1024,...).

Następnie należy odszyfrować kryptogram i zaobserwować powstałe zmiany w tekście jawnym.

**Pytania/Wnioski:**

### Czy i jak długość klucza wpływa na entropię TT?

### Czy i jak długość klucza wpływa na autokorelację TT?

### Czy i jak obserwowana entropia TT zależy od entropii TJ?

### Jak kształtuje się czas szyfrowania/deszyfrowania w zależności od długości pliku.

### Jak wygląda czas operacji szyfrowania/deszyfrowania algorytmem asymetrycznym w porównaniu do realizacji tych operacji algorytmem symetrycznym.

### Jak wyglądają zmiany w TJ przy wprowadzeniu przekłamań do TT? Jaka ich jest skala? Od czego zależy?

### Czy można usunąć fragment z TT tak, aby pozostały tekst TJ po odszyfrowaniu był czytelny?

### Jakie są wady i zalety algorytmów asymetrycznych w porównaniu do algorytmów symetrycznych?

### W jakich zastosowaniach lepiej korzystać algorytmów asymetrycznych, a w jakich z algorytmów symetrycznych?

# Raport z przeprowadzonych eksperymentów.

Raport powinien mieć postać dokumentu elektronicznego, w którym zostanie zapisany przebieg realizowanych w trakcie zajęć eksperymentów (np. fragment treści tekstu jawnego, parametry algorytmu szyfrowania, fragment kryptogramu) oraz wnioski, spostrzeżenia, odpowiedzi na pytania umieszczone w instrukcji laboratoryjnej, itp.