

I. Temat zadania: Kryptosystemy z kluczem prywatnym – internetowy serwis edukacyjny

II. Plan pracy:

1. Przegląd literatury dotyczącej systemów szyfrowania danych z kluczem prywatnym.
 2. Zapoznanie z wybranymi zagadnieniami polityki bezpieczeństwa w sieci Internet dotyczącej kryptosystemów z kluczem prywatnym (m.in. metody autoryzacji użytkowników, zarządzanie kluczami prywatnymi).
 3. Przegląd literatury dotyczącej tworzenia interaktywnych serwisów internetowych.
 4. Projekt i realizacja internetowego serwisu edukacyjnego poświęconego systemom szyfrowania danych z kluczem prywatnym.
 5. Wnioski.

III. Cel pracy Celem pracy jest zaprojektowanie i realizacja internetowego serwisu edukacyjnego poświęconego systemom szyfrowania danych z kluczem prywatnym.

I. Temat zadania: Kryptosystemy z kluczem publicznym – internetowy serwis edukacyjny

II. Plan pracy:

1. Przegląd literatury dotyczącej systemów szyfrowania danych z kluczem publicznym.
 2. Zapoznanie z wybranymi zagadnieniami polityki bezpieczeństwa w sieci Internet dotyczącej kryptosystemów z kluczem publicznym (m.in. certyfikaty bezpieczeństwa, metody autoryzacji użytkowników, zarządzanie kluczami publicznymi).
 3. Przegląd literatury dotyczącej tworzenia interaktywnych serwisów internetowych.
 4. Projekt i realizacja internetowego serwisu edukacyjnego poświęconego systemom szyfrowania danych z kluczem publicznym.
 5. Wnioski.

III. Cel pracy Celem pracy jest zaprojektowanie i realizacja internetowego serwisu edukacyjnego poświęconego systemom szyfrowania danych z kluczem publicznym.

I. Temat zadania: Analiza bezpieczeństwa kryptosystemu RSA – program komputerowy

II. Plan pracy:

1. Przegląd literatury dotyczącej systemów szyfrowania danych z kluczem publicznym.
 2. Przegląd literatury dotyczącej kryptoanalizy systemów szyfrowania danych z kluczem publicznym.
 3. Przegląd metod komputerowych implementacji algorytmów, realizujących operacje stałoprzecinkowe z wykorzystaniem bardzo dużych liczb całkowitych.
 4. Projekt programu komputerowego poświęconego analizie bezpieczeństwa kryptosystemu RSA.
 5. Realizacja programu komputerowego z pkt. 4 z wykorzystaniem języka C/C++.
 6. Wnioski.

III. Cel pracy Celem pracy jest zaprojektowanie i realizacja programu komputerowego poświęconego analizie bezpieczeństwa kryptosystemu RSA.