Bezpieczeństwo danych i elementy kryptografii

Instytut Automatyki, Elektroniki i Elektrotechniki,
Wydział Informatyki, Elektrotechniki i Automatyki, Uniwersytet Zielonogórski

przygotował: *dr hab. inż. Remigiusz Wiśniewski, prof. UZ*

ZAKRES TEMATYCZNY PRZEDMIOTU

1. Podstawowe mechanizmy szyfrowania danych, bezpieczeństwo systemów danych w informatyce, zastosowanie kryptografii w życiu codziennym (podpis elektroniczny, szyfrowanie haseł w Informatyce, zabezpieczenia kart elektronicznych, itd.).
2. Podstawowe algorytmy kryptograficzne (podstawieniowe, mono- i polialfabetyczne).
3. Algorytmy szyfrowania symetrycznego: ogólna charakterystyka, zastosowanie, sposób realizacji z wykorzystaniem języków programowania (C, C++, C#, Assembler, Pascal), algorytmy szyfrowania blokowego (DES, AES) oraz strumieniowego (RC4).
4. Algorytmy szyfrowania asymetrycznego: ogólna charakterystyka, zastosowanie w praktyce.
5. Jednokierunkowe funkcje skrótu, zastosowanie w serwisach internetowych.
6. Podpis elektroniczny: ogólna charakterystyka, zastosowanie, podstawowe własności oraz mechanizmy. Podpis tradycyjny, a podpis elektroniczny; podobieństwa, różnice, porównanie pod kątem bezpieczeństwa i wiarygodności.
7. Kryptoanaliza: Wprowadzenie i omówienie podstawowych założeń kryptoanalizy. Zastosowanie mechanizmu analizy (ang. debugging) programów komputerowych w kryptoanalizie.
8. Bezpieczeństwo serwisów Internetowych, analiza najpopularniejszych ataków (m.in. SQL-Injection, Cross-site Scripting). Zabezpieczenia serwisów Internetowych na poziomie bazy, aplikacji, serwera.
9. Kryptografia praktyczna: Podstawowe metody ochrony kont Internetowych (np. kont pocztowych, bankowych, czy profili w serwisach społecznościowych). Praktyczne sposoby doboru haseł, przydatne narzędzia wspomagające ochronę danych w życiu codziennym (m.in. ukrywanie dysków, czy partycji, prosta i szybka archiwizacja danych z wykorzystaniem mechanizmów systemowych.

WARUNKI ZALICZENIA LABORATORIUM, WYKŁADU ORAZ PROJEKTU

1. Warunkiem zaliczenia laboratorium jest uzyskanie pozytywnej oceny z:
   a. zadań wykonywanych na zajęciach;
   b. pisemnego sprawdzenia wiadomości (tzw. „wejściówki”);
   c. sprawozdania z wykonanego ćwiczenia.
2. Podstawą zaliczenia laboratorium jest zaliczanie wszystkich ćwiczeń laboratoryjnych.
3. Warunkiem zaliczenia wykładu jest uzyskanie pozytywnej oceny z wszystkich kolokwiów.
4. Każde kolokwium zostanie wcześniej zapowiedziane przez prowadzącego zajęcia.
5. Sposób przeprowadzenia oraz liczbę kolokwiów w semestrze ustala prowadzący zajęcia.
6. W uzasadnionych przypadkach istnieje możliwość zwolnienia studenta z kolokwium, przy czym każdy student musi napisać i zaliczyć przynajmniej jedno kolokwium.
7. Warunkiem zaliczenia projektu jest poprawne, rzetelne i terminowe wykonywanie wszystkich zadań projektowych, zadanych przez prowadzącego zajęcia.
8. Opóźnienie oddania projektu lub sprawozdania z laboratorium skutkuje automatycznym obniżeniem o ocenę w dół za każdy tydzień opóźnienia.

LITERATURA

[1] Stinson D.R., *Kryptografia*, WNT, Warszawa, 2005.
[2] Karbowski M., *Podstawy Kryptografii*, Helion, Warszawa, 2005.
[3] Schneier B., *Kryptografia dla praktyków*, WNT, Warszawa, 2002.
[4] Aho A. V., Hopcroft J. E., Ullman J. D., *Algorytmy i struktury danych*. Helion, Warszawa, 2003.
[5] Strona internetowa https://niebezpiecznik.pl (dostęp: 29.09.2018).
[6] Strona internetowa https://zaufanatrzeciastrona.pl (dostęp: 29.09.2018).