ВЕРОЯТЕН КОНСПЕКТ

ВЪВЕДЕНИЕ В КРИПТОГРАФИЯТА И СИГУРНОСТТА НА ДАННИТЕ

проф. д.т.н. Веселин Целков

Университет по библиотекознание и информационни технологии

Комисия за защита на личните данни

Сигурност на данните

1. Модел на заплахите за сигурността
2. Осигуряване на сигурността на ИТ
3. Модел на услугите за сигурност
4. Направления и услуги за сигурност

Криптографски алгоритми

5. Криптографски алгоритми. Основни понятия
6. Цифров подпис
7. Криптографски услуги и механизми. Сигурност на криптосистема
8. Управление на криптографските ключове

Класическа криптография

9. Основни методи:

- Заместване (субституция)
    - Брой азбуки

        - Една азбука
        - Много азбуки
    - Брой букви
        - Една буква
        - Много букви
- Разместване (пермутация)

10. Методи базирани на заместване

- Атбаш I -> n – I + 1 (иврит)
- Квадрат Полибия
- Цезар
- Произволна пермутация. Честотен анализ
    - На буквите
    - На съчетанията от букви (двубучия, трибучия и т.н.)
    - Най-често срещани думи
- Много буквено криптиране
    - Шифърът на Плейфеър
    - Хил шифър
- Много азбучни шифри
    - Вижинер

11. Методи базирани на разместване

- Rail-Fence метод
- Шифър Ред-стълб
- Двоен Ред-стълб
- Роторни машини

- Криптомашина Енигма

Съвременна криптография

12. Модерни блокови шифри. Схема на Фейстел
13. Модерни блокови шифри. DES
14. Модерни блокови шифри. AEC
15. Асиметрични криптосистеми (криптосистеми с публичен ключ)
16. Криптосистема RSA
17. Криптосистема ElGamal
18. Цифров подпис

ноември 2015 г

гр. София **проф. д.т.н. ВЕСЕЛИН ЦЕЛКОВ**