Wykład 5

Temat: Wspólne sekrety i tajne klucze, czyli wstęp do kryptografii

KAPITAŁ LUDZKI
CZŁOWIEK – NAJLEPSZA INWESTYCJA!

Projekt *„Przygotowanie i realizacja kierunku inżynieria biomedyczna – studia międzywydziałowe”*
współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego. Nr umowy UDA – POKL.04.01.01-00-236/08

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Dlaczego potrzebujemy kryptografii?

- potwierdzenie tożsamości
- poufność transmisji
- zabezpieczenie danych przed kradzieżą
- pewność poprawności danych/komunikatu

Projekt *„Przygotowanie i realizacja kierunku inżynieria biomedyczna – studia międzywydziałowe”*
współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego. Nr umowy UDA – POKL.04.01.01-00-236/08

- symetryczna:
    - może być blokowa lub strumieniowa
    - jeden klucz do szyfrowania i odczytu (wada)
    - mniej wymagająca obliczeniowo (wada i zaleta)
- asymetryczna:
    - oddzielne klucze do szyfrowania i odczytu
    - komplikacja rośnie wraz z mocą komputerów
    - podstawa dzisiejszej informatyki i telekomunikacji
    - pozwala na potwierdzenie autentyczności komunikatu
    - hierarchia poświadczeń kluczy
- funkcja (prawie)jednokierunkowa:
    - w założeniach bezpowrotnie niszczy informacje
    - tworzy 'odcisk' informacji o stałej długości

Projekt *„Przygotowanie i realizacja kierunku inżynieria biomedyczna – studia międzywydziałowe”*
współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego. Nr umowy UDA – POKL.04.01.01-00-236/08

Kryptografia w informatyce

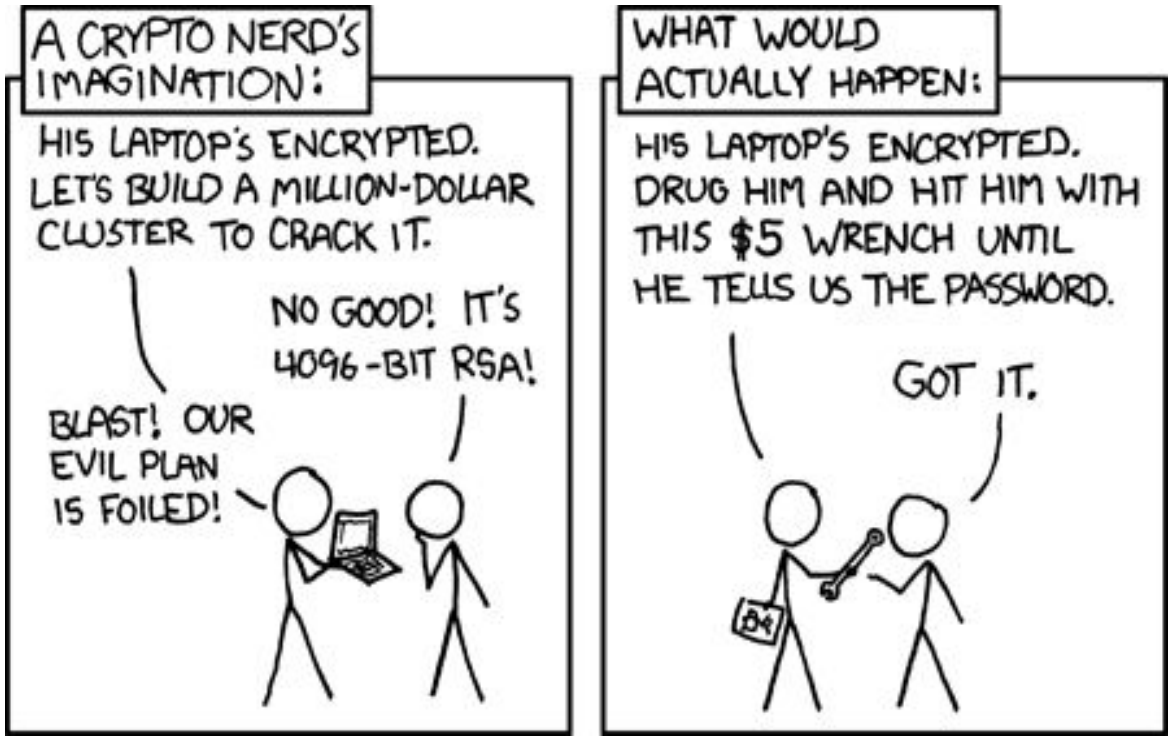
- symetryczna: DES, AES, RC4
    - szyfrowanie dysków/plików
    - poufność transmisji
- asymetryczna: DSA, RSA
    - poczta elektroniczna
    - nawiązywanie bezpiecznego kanału komunikacji
    - podpis kwalifikowany
    - autentyczność kodu programu
    - poświadczenie tożsamości
- funkcje jednokierunkowe: MD5, SHA1, SHA512
    - kontrola integralności plików
    - przechowywanie haseł
    - deduplikacja

KAPITAŁ LUDZKI
CZŁOWIEK – NAJLEPSZA INWESTYCJA!

Projekt *„Przygotowanie i realizacja kierunku inżynieria biomedyczna – studia międzywydziałowe”*
współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego. Nr umowy UDA – POKL.04.01.01-00-236/08

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Słaba strona kryptografii



Z xkcd.com

Projekt *„Przygotowanie i realizacja kierunku inżynieria biomedyczna – studia międzywydziałowe”*
współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego. Nr umowy UDA – POKL.04.01.01-00-236/08

Certyfikaty klucza publicznego

Typowy certyfikat ma postać podpisanego cyfrowo pliku. Plik ten poza informacjami technicznymi zawiera, także:
- informację o tym kto wydał dany certyfikat
- od i do kiedy jest on ważny
- możliwe przypadki użycia (poświadczenie tożsamości, podpisywanie dokumentów)
- informację czyją tożsamość potwierdza
- odcisk klucza publicznego powiązanego z kluczem prywatnym

Organ wydający certyfikat jest trzecią gwarantującą tożsamość podmiotu posługującego się certyfikatem.

KAPITAŁ LUDZKI
CZŁOWIEK – NAJLEPSZA INWESTYCJA!

Projekt *„Przygotowanie i realizacja kierunku inżynieria biomedyczna – studia międzywydziałowe”*
współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego. Nr umowy UDA – POKL.04.01.01-00-236/08

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY