Bezpieczeństwo Systemów Komputerowych
Projekt 1 – opis zadań

dr inż. Piotr Rajchowski

POLITECHNIKA GDAŃSKA

- **Szyfry blokowe:**
- **AES** (Rijndael) – trzy wielkości bloku: 128, klucza: 128/192/256 bitów; wykonywany w rundach
- **DES** – wielkość bloku: 64 bity, klucza: 56 bitów; wykonywany w 16 turach
- **3DES** – potrójny DES, trzy realizacje: EEE, EDE (3 niezależne klucze), EDE (2 niezależne klucze)
- **Blowfish** – wielkość bloku: 64 bity, klucza do 448 bitów; wykonywany w 16 rundach

POLITECHNIKA GDAŃSKA

- **Tryby pracy szyfrów blokowych:**
- **ECB** – *Electronic Code Book* – dzielenie wiadomości na podbloki o długości dostosowanej dla danego algorytmu szyfrującego.
- **CBC** – *Cipher Block Chaining* – dane wejściowe kolejnego bloku są zależne od wyjścia bloku poprzedzającego. Blok szyfrogramu nie jest zależny od bloku tekstu jawnego trafiającego do kolejnego bloku. Tekst jawny jest łączony z wektorem inicjującym.
- **CFB** – *Cipher Feedback Mode* – dane wejściowe kolejnego bloku są zależne od wyjścia bloku poprzedzającego (również od tekstu jawnego). Blok szyfrogramu jest zależny od bloku tekstu jawnego. Tekst jawny nie jest łączony z wektorem inicjującym a z szyfrogramem.
- **OFB** – *Output Feedback Mode* – dane wejściowe kolejnego bloku są zależne od wyjścia bloku poprzedzającego. Szyfrogram stanowi wejście kolejnego bloku szyfrującego (niezależny od bloku tekstu jawnego)

- **Interfejs użytkownika powinien umożliwiać swobodny wybór pliku wejściowego oraz wybór nazwy pliku wynikowego**

- Program ma umożliwiać wybranie dowolnego pliku (*.txt, *.png, *.mp3, *.avi, itp.) z dowolnej lokalizacji
- Należy zwrócić uwagę na rozmiar pliku wejściowego – program ma umożliwiać wybór plików o rozmiarze nawet kilkuset MB. Konieczne jest przedstawienie procentowego postępu procesu szyfrowania.
- Aplikacja deszyfrująca (jest to druga funkcja wykonanej aplikacji) na podstawie pliku wejściowego (o przyjętej strukturze) odtwarza plik poddany procesowi szyfrowania z możliwością modyfikacji nazwy podtrzymując jego rozszerzenie

POLITECHNIKA GDAŃSKA

- **Możliwy jest wybór jednego z czterech trybów szyfrowania: ECB,CBC,CFB,OFB**

- Użytkownik ma mieć możliwość wyboru trybu szyfrowania np. korzystając z rozwijanej listy a informacja o wybranym trybie ma być umieszczona w sposób jawny w pliku wynikowym
- Podczas deszyfrowania tryb szyfrowania oraz pozostałe dane wejściowe algorytmu powinny być wybierane automatycznie.

- **Dla trybu CFB i OFB podczas wyboru długości podbloku mniejszego od długości bloku algorytmu kolejne długości podbloku powinny być potęgą liczby 2 lub wielokrotnością bajtu**

POLITECHNIKA GDAŃSKA

- **Należy opracować (zaadaptować) strukturę pliku wynikowego.**

- ***Zawartość*** pliku musi być przekazana w postaci zaszyfrowanej.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<EncryptedFileHeader>
        <Algorithm>nazwa</Algorithm>
        <KeySize>rozmiar</KeySize>
        <BlockSize>rozmiar</BlockSize>
        <CipherMode>tryb</CipherMode>
        <IV>wektor_początkowy</IV>
        <ApprovedUsers>
                <User>
                <Email>identyfikator użytkownika</Email>
                <SessionKey>zaszyfrowany klucz sesyjny</SessionKey>
                </User>
                …
        </ApprovedUsers>
</EncryptedFileHeader>
Zaszyfrowane dane
```

- **Należy dobrać dobrej jakości generatory pseudolosowe do generowania kluczy sesyjnych. Wartością początkową generatora powinny być przypadkowe ciągi binarne pobrane z otoczenia, np. aktualny czas systemowy (32 lub 64 bity), numer sektora dyskowego z ostatniej transmisji, wskazanie kursora myszki, itp.**

- Generatory pseudolosowe mają na celu dostarczenie danych wejściowych w celu wygenerowania kluczy danego (każdego) użytkownika. Liczba wygenerowanych kluczy musi być równa liczbie dozwolonych użytkowników.
- Należy przyjąć, że aplikacja powinna obsługiwać nie mniej niż 5 użytkowników.

- Kolejnym krokiem jest wygenerowanie pary kluczy (klucza publicznego oraz klucza prywatnego) z użyciem algorytmu RSA.

- **Klucz sesyjny powinien być zaszyfrowany kluczem publicznym RSA zamierzonego odbiorcy.**
- **Należy pamiętać, że w przypadku użycia RSA do transportu klucza sesyjnego może wystąpić większa liczba odbiorców tego samego szyfrogramu.**
- **Klucze prywatne i publiczne powinny być przechowywane oddzielnie (w odrębnych katalogach).**

- Szyfrowanie kluczy powinno odbywać się w sposób półautomatyczny – użytkownik wyzwala generowanie klucza sesyjnego, następnie wygenerowana zostaje para kluczy (z których jeden zostaje zaszyfrowany), a w ostatnim etapie klucze zapisywane są ustalonej lokalizacji. Użytkownik nie może wskazywać miejsca zapisania kluczy.

- **Jako że w aplikacji zastosowano algorytm RSA przed procesem deszyfracji istnieje konieczność przejrzenia listy potencjalnych odbiorców pliku (szyfrogramu). Odbiorca szyfrogramu powinien wskazać siebie na tej liście i na tej podstawie automatycznie jego nazwa powinna zostać powiązana z kluczem prywatnym przechowywanym w dedykowanym katalogu.**

- W przypadku nieautoryzowanej próby deszyfracji aplikacja nie może informować użytkownika o braku uprawnień do chronionej treści.

POLITECHNIKA GDAŃSKA

- **W przypadku użycia RSA klucze prywatnie muszą być przechowywane w postaci zaszyfrowanej w trybie ECB, a kluczem szyfrującym jest skrót* hasła dostępu do klucza prywatnego danego użytkownika *(np. uzyskanym z hasła za pomocą funkcji SHA-1, SHA-256 lub innej dobrej jakości funkcji skrótu). Użyta funkcja skrótu musi być wskazana w dokumentacji projektu.**

- Do szyfrowania klucza prywatnego należy użyć wybranego szyfru blokowego.
- Użytkownik może utworzyć dowolne hasło dostępu o dowolnej (rozsądnej) długości.
- Obligatoryjne jest zaimplementowanie podstawowej analizy wprowadzanego hasła (minimalna długość osiem znaków; hasło dostępu musi składać się z co najmniej: jednej cyfry, jednej litery, jednego znaku specjalnego).

POLITECHNIKA GDAŃSKA

- **Należy użyć implementacji algorytmów szyfrowania dostępnych w Internecie.**

- W wytworzonej dokumentacji projektowej obligatoryjne jest wskazanie źródeł zastosowanych składników.