E-MEDIA — PROJEKT 2

Szyfrowanie danych algorytmem RSA

Andrzej Gnatowski 8 marca 2022

1 Wymagania projektowe

- Napisać program do szyfrowania i deszyfracji pliku multimedialnego algorytmem RSA.
- Zaszyfrować wyłącznie masę bitową pliku, pozostawiając nagłówek i metadane bez zmian — plik zaszyfrowany musi się dać otworzyć standardowymi aplikacjami, ale jego zawartość powinna być zakodowana (zaszyfrowana). W razie konieczności modyfikacji metadanych, proszę uzasadnić dokonany wybór.

  Uwaga! Dla niektórych formatów plików identyfikacja które fragmenty są danymi, a które metadanymi może być trudne. W razie wątpliwości, proszę pytać.
- Dla plików wykorzystujących kompresję, należy przetestować (o ile to możliwe):
  - szyfrowanie zdekompresowanych danych, a następnie skompresowanie tak utworzonego szyfrogramu;
  - bezpośrednie szyfrowanie skompresowanych danych.

  Czy obie metody są równoważne?
- Metodę szyfrującą i deszyfrującą należy napisać samodzielnie, bez użycia bibliotek szyfrujących. Można skorzystać z gotowych bibliotek do:
  - obliczeń na dużych liczbach (w tym przeprowadzania operacji potęgi modulo);
  - generowania liczb pierwszych;
  - generowania liczb losowych.
- Operację szyfrowania przeprowadzić wykorzystując *Electronic CodeBook* oraz co najmniej jedną, inną metodę.
- Ocenić, czy informacje są możliwe do odczytania po zaszyfrowaniu (np. czy widać zarys obiektu dla ECB).
- Skorzystać z gotowej funkcji szyfrującej metodą RSA. Szyfrować tą samą parą kluczy. Porównać wynik szyfrowania z rezultatami implementowanych algorytmów.
- Podjąć próbę wyjaśnienia przyczyny ewentualnych wyraźnych różnic.

2 Sposób zaliczenia

1. Grupa projektowa prezentuje program oraz uzasadnia podjęte decyzje (w szczególności w zakresie ewentualnej modyfikacji metadanych).
2. Rozmowa na temat kodu (ma na celu sprawdzenie znajomości jego zasady działania).
3. Opcjonalny test programu na losowych danych.
4. Rozmowa na temat znaczenia wyboru systemu kryptograficznego, w kontekście wybranego formatu multimediów.
5. Udostępnienie prowadzącemu kodu źródłowego projektu w celach archiwizacyjnych.

3 Pozostałe informacje

- Preferowane jest pozostanie w tej samej grupie co w przypadku projektu 1.
- Silnie preferowane jest pozostanie przy tym samym formacie plików multimedialnych co w projekcie 1.
- Można używać dowolnego języka programowania.
- Program nie musi mieć GUI, ale nie warto się bać tego elementu — nie ma wymagań dotyczących ergonomii i estetyki.