Informacje

- **Kontakt:** katarzyna.mazur@umcs.pl
- **Konsultacje:** pokój 412 na 4 piętrze, przed konsultacjami proszę o wiadomość mailową
- **Zasady zaliczenia:** `https://kampus.umcs.pl/pluginfile.php/806844/mod_resource/content/1/zasady_zaliczenia_bsk_2022.pdf`
- **Materiały, aktualności, zmiany terminów zajęć:** `https://kampus.umcs.pl/course/view.php?id=20754`

Zadania

2.1 Wykonaj szyfrowanie ciągu znaków z pliku `ex2.1.txt` za pomocą algorytmu AES-256-ECB z użyciem podanego klucza. Klucz znajduje się w pliku `ex2.1.key`. Odpowiedź (zaszyfrowany tekst) zakoduj kodowaniem Base64. Klucz użyty podczas szyfrowania powinien być podawany z linii komend. Prawidłowa odpowiedź do zadania znajduje się w pliku `ex2.1.enc`.

2.2 Wykonaj deszyfrowanie pliku `ex2.2.enc` za pomocą algorytmu AES-256-ECB z użyciem podanego klucza z pliku `ex2.2.key`. Klucz powinien być podawany w linii komend. Wynikiem powinien być zrozumiały tekst.

2.3 Wykonaj deszyfrowanie pliku `ex2.3.enc` za pomocą algorytmu CAMELLIA-128-ECB z użyciem podanego hasła z pliku `ex2.3.key`. Hasło powinno być podawane z pliku.

2.4 Wykonaj deszyfrowanie pliku `ex2.4.enc` za pomocą algorytmu AES-256-CBC z użyciem podanego hasła z pliku `ex2.4.pass`, wiedząc, że funkcja generowania klucza to PBKDF2.

2.5 Wykonaj deszyfrowanie pliku `ex2.5.enc` za pomocą algorytmu 3DES z użyciem podanego klucza z pliku `ex2.5.key`, wiedząc, że funkcja generowania klucza to PBKDF2.

2.6 Wykonaj szyfrowanie pliku `ex2.6.txt` za pomocą algorytmu BLOWFISH-ECB z użyciem klucza, który wygenerujesz za pomocą `OpenSSL rand`. Następnie wykonaj deszyfrowanie pliku, zapisując wynik deszyfrowania do pliku `ex2.6.dec`. Za pomocą polecenia `diff` lub `md5sum` sprawdź, czy pliki `ex.2.6.txt` oraz `ex2.6.dec` są identyczne.

2.7 Wykonaj deszyfrowanie pliku `ex2.7.enc` za pomocą algorytmu AES-256-ECB z użyciem podanego klucza z pliku `ex2.7.key`, algorytmu generowania klucza PBKDF1 oraz wskazanej ilości iteracji algorytmu równej 356.

2.8 Wykonaj deszyfrowanie pliku `ex2.8.txt` za pomocą algorytmu AES-256-CBC z użyciem podanego hasła z pliku `ex2.8.pass`, algorytmu generowania klucza PBKDF2 oraz wskazanej ilości iteracji algorytmu równej 41331.

2.9 Ze strony kursu pobierz plik `ex2.9.zip`. Plik ten jest zabezpieczony hasłem. Jest to jedno z najczęściej używanych przez użytkowników haseł. Za pomocą programu JohnTheRipper spróbuj złamać hasło, którym zaszyfrowany jest plik. Możesz skorzystać z listy najpopularniejszych haseł dostępnej na githubie: `https://raw.githubusercontent.com/danielmiessler/SecLists/master/Passwords/Common-Credentials/10k-most-common.txt`.

2.10 Ze strony kursu pobierz plik `ex2.10.zip`. Plik ten jest zabezpieczony hasłem. Wiedząc, że plik ten jest zabezpieczony hasłem o długości pomiędzy 5-6 znaków, i zawiera jedynie cyfry, za pomocą programu JohnTheRipper spróbuj złamać hasło, którym zaszyfrowany jest plik. Wygeneruj listę możliwych haseł za pomocą programu `crunch`.

2.11 Wykonaj zadanie **2.9** za pomocą narzędzia `fcrackzip`.

2.12 Zidentyfikuj, jaki algorytm szyfrujący został wykorzystany do zaszyfrowania tekstu: `Z8CerTOLe1JlDKWfvDeifw==` przy pomocy klucza: `a35febba42490abe`.

2.13 W pliku `ex2.13.txt` znajduje się zaszyforwany za pomocą klucza z pliku `ex2.13.key` obrazek w formacie `*.png`. Odszyfruj obrazek. Rozwiązaniem zadania powinien być plik `*.png`. Do szyfrowania obrazka użyto algorytmu SEED-ECB.

2.14 Ze strony kursu pobierz plik `ex2.14.zip`. Plik ten jest zabezpieczony hasłem. Spróbuj złamać hasło za pomocą narzędzia `hashcat` wykorzystując atak słownikowy.

Linki

- `https://www.openssl.org/docs/man1.0.2/man1/openssl-enc.html`
- `https://wiki.openssl.org/index.php/Enc`