ZAD1

Zahaszuj słowo **Linux** za pomocą algorytmu MD5.

ZAD2

Zahaszuj słowo **Linux** za pomocą algorytmu SHA-256.

ZAD3

Zakoduj słowo **Linux** za pomocą kodowania base64.

ZAD4

Odkoduj słowo **VU1DUw==** zakodowane za pomocą base64.

ZAD5

Zaszyfruj słowo **Linux** za pomocą algorytmu AES-256-ECB i klucza **e592bc9e5fa8618a02edf437bdf3ffd4fcdfbe9e588749db898a3662b461a80e**.

ZAD6

Zaszyfruj słowo Linux za pomocą AES-256-CFB, klucza **e592bc9e5fa8618a02edf437bdf3ffd4fcdfbe9e588749db898a3662b461a80e** oraz IV **83c468dc477543a6906912b6a1344416.**

ZAD7

Zaszyfruj słowo **Linux** za pomocą AES-256-CFB, klucza **e592bc9e5fa8618a02edf437bdf3ffd4fcdfbe9e588749db898a3662b461a80e** oraz IV **83c468dc477543a6906912b6a1344416.** Wynik szyfrowania zakoduj za pomocą kodowania base64.

ZAD8

Słowo **f6NB8w==** zostało zaszyfrowane algorytmem AES-256-CFB, kluczem **e592bc9e5fa8618a02edf437bdf3ffd4fcdfbe9e588749db898a3662b461a80e** oraz IV **83c468dc477543a6906912b6a1344416**, a następnie zakodowane za pomocą kodowania base64. Odszyfruj i odkoduj słowo.

ZAD9

Wygeneruj klucz szyfrujący o długości 128 bitów.

ZAD10

Zaszyfruj słowo **Linux** za pomocą AES-128-CBC, bez soli, hasło do generowania klucza to **Ubuntu**, funkcja generowania klucza to PBKDF2, z liczbą iteracji równą 256.

ZAD11
Wygeneruj parę kluczy (publiczny i prywatny), klucze mają 2048 bitów. Wyeksportuj klucze do pliku.

ZAD12
Wygeneruj parę kluczy (publiczny i prywatny), klucze mają 2048 bitów. Wyeksportuj klucze do pliku. Zaszyfruj słowo **Linux** kluczem publicznym i odszyfruj prywatnym. Użyj paddingu OAEP.

ZAD13
Wygeneruj parę kluczy (publiczny i prywatny), klucze mają 2048 bitów. Wyeksportuj klucze do pliku. Zapisz do pliku słowo **Linux**. Podpisz plik używając klucza prywatnego, z paddingiem PSS: hash SHA-256, długość soli powinna odpowiadać długości funkcji skrótu. Zweryfikuj wygenerowany podpis.

ZAD14
Złam hash MD5: **e2fc714c4727ee9395f324cd2e7f331f** za pomocą:

1) ataku słownikowego,
2) generując swój własny słownik, widząc, że hasło ma 4 znaki i składa się z małych liter a-z
3) za pomocą maski, widząc, że hasło ma 4 znaki i składa się z małych liter a-z

ZAD15
Wygeneruj parę kluczy GPG dla maila student@umcs.pl. Klucz RSA, 1024 bity. Wyeksportuj klucz publiczny i prywatny do pliku.

ZAD16
Zaszyfruj słowo Linux algorytmem AES z kluczem 128 bitów, z hasłem Ubuntu używając GPG. Wynik zapisz do pliku. Odszyfruj plik.

ZAD17
Wygeneruj parę kluczy RSA (GPG) z domyślnymi parametrami. Zaszyfruj słowo **Linux** przy użyciu klucza publicznego. Wynik szyfrowania zapisz do pliku. Odszyfruj plik.

ZAD18
Wygeneruj parę kluczy RSA (GPG) z domyślnymi parametrami. Zapisz słowo **Linux** do pliku, podpisz plik przy użyciu klucza publicznego. Użyj kodowania base64. Wynik podpisywania zapisz do pliku. Zweryfikuj podpisany plik.

ZAD19
Uruchom serwer i przetesuj wysyłanie do serwera pliku / tekstu:

podman run -p 5000:5000 docker.io/mazurkatarzynaumcs/echoserver:latest
docker run -p 5000:5000 docker.io/mazurkatarzynaumcs/echoserver:latest