Autor: Maciej Milewski 17947
Michał Degowski 16584

Algorytmy szyfrujące - raport

Do pomiaru czasu pracy algorytmów został wykorzystany moduł timeit
https://docs.python.org/3/library/timeit.html

Dane wejściowe zostały wygenerowane na stronie:
https://www.lipsum.com/feed/html

Dla 5000 wygenerowanych słów użytych jako dane wejściowe do szyfrowania otrzymaliśmy następujące wyniki:

Algorytm	Czas szyfrowania	Czas deszyfrowania
DES	2.2294297 s	2.1873590999999997 s
3DES	8.705938699999997 s	8.874385699999998 s
AES	0.0044821 s	0.00037629999999999955 s
ElGamal	0.9100368 s	1.6567357999999999 s
ECC & AES	0.07253980000000126 s	0.035727399999998966 s

Rekomendacje:

Dla kryptografii asymetrycznej warto skorzystać z algorytmu ECC. Jest zdecydowanie szybszy od rozwiązania ElGamal. Ponadto dostępne implementacje zapewniają wysoki poziom bezpieczeństwa - dorównujący RSA. W przypadku szyfrów symetrycznych rozwiązanie AES bezkonkurencyjnie wygrywa z 3DES oraz przestarzałym DES. Duży wpływ na szybkość obliczeń ma również wybór biblioteki. Najpopularniejsze rozwiązania, takie jak moduł PyCrypto są dużo lepiej zoptymalizowane od mniej popularnych implementacji.