Rok akademicki	Termin	Kierunek	Prowadzący	Grupa	Sekcja
2013/2014	Poniedziałek P	INF 2 SSM	dr inż. Jacek Lach	OS1	1
8:00 – 10:00					

Laboratorium Zaawansowanych Metod Kryptograficznych

Sprawozdanie z ćwiczenia numer 2

Data wykonania ćwiczenia 17.03.2014

Temat ćwiczenia:

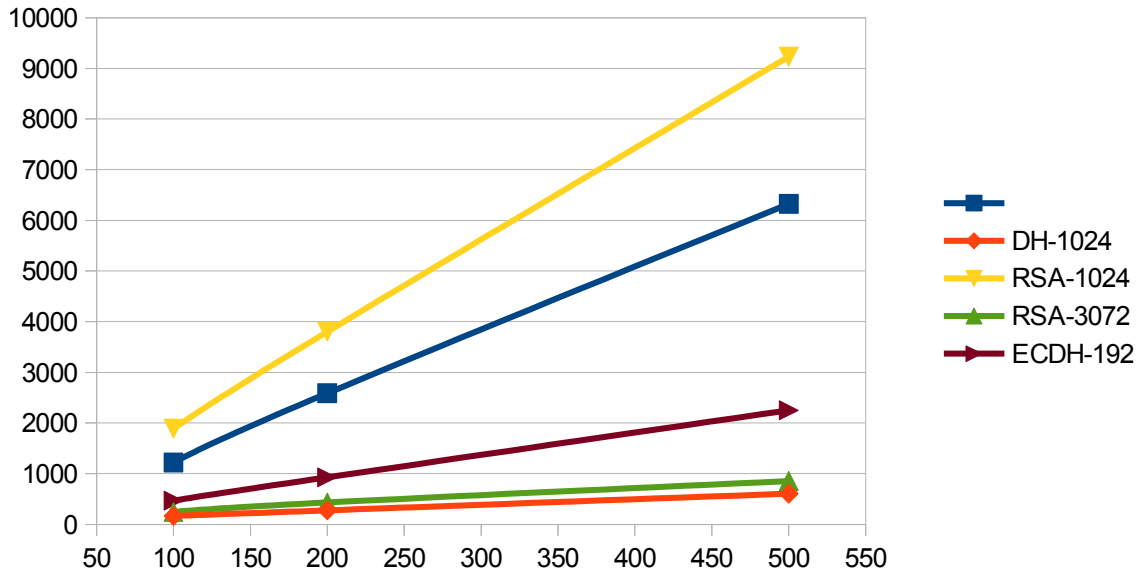
Uzgadnianie klucza

Skład podsekcji:
Marius Rejdak

Pomiary czasów

Liczba wymian klucza	100	200	500
DH-1024	1222	2588	6327
RSA-1024	165	277	606
RSA-3072	1888	3803	9231
ECDH-192	244	432	855
ECDH-256	469	928	2252

Jednostka czasu: ms



Analiza wyników

Logiczne wydaje się porównywanie kluczy o podobnym bezpieczeństwie, zatem należałoby porównać ze sobą RSA-1024 z ECDH-192, a RSA-3072 z ECDH-256. W przypadku mniejszej wielkości klucza lepszy wydaje się algorytm RSA, lecz nie jest to znacząca różnica, zaś dla większych kluczy rozbieżność już jest ogromna i wygrywa tutaj ECDH. Można się spodziewać że w przyszłości algorytmy oparte o ECC będą coraz częściej wykorzystywane, gdyż wraz ze wzrostem wielkości klucza ich złożoność obliczeniowa nie rośnie tak szybko jak w algorytmie RSA.