Politechnika Warszawska

Wydział Fizyki

Kryptografia i bezpieczeństwo informacji dla fizyków

Sprawozdanie z zadania nr. 3 na temat:

Konsekwencje braku losowości: generacja kluczy RSA

Data wykonania zadania w laboratorium: 05.11.2019r.

Wykonali:

Maciej Czarnecki

Denys Morokov

Fizyka techniczna II stopień, 2 rok

1. Wstęp

1.1. Cel: celem zadania jest na pisanie prostego skryptu do ściągania kluczy publicznych wybranych domen oraz porównywania tych kluczy. Lista wykorzystanych domen znajduje się w pliku .XML dołączonym do sprawozdania.

1.2. Wykorzystana technologia:

Skrypt został napisany w języku python z wykorzystaniem biblioteki OpenSSL

2. Podsumowanie

Nie wykryliśmy duplikatów klucza publicznego w większości domen. Wyjątkiem był jedynie przypadek www.google.pl i www.youtube.pl . Prawdopodobnie spowodowane jest to tym że youtube jest częścią googla i obie witryny korzystają z tych samych kluczy.