

Politechnika Warszawska
Wydział Fizyki
Kryptografia i bezpieczeństwo informacji dla fizyków

Sprawozdanie z zadania nr. 4 na temat:

Faktoryzacja kluczy RSA – wg. Bernstein, Heringer, Lange

Data wykonania zadania w laboratorium: 12.11.2019r.

Wykonali:

Maciej Czarnecki

Denys Morokov

Fizyka techniczna II stopień, 2 rok

1. Wstęp

1.1. Cel: celem zadania napisanie prostego crawler'a do kluczy, który dla zadanej listy domen ściągnie ich klucze publiczne (otrzymane w poprzednim zadaniu 3) i sprawdzi metodą batchGCD czy da się odtworzyć klucze prywatne.

1.2. Wykorzystana technologia: skrypt z zaimplementowaną metodą batchGCD został napisany w Sage, który jest systemem algebry komputerowej napisanej w Pythonie (<http://www.sagemath.org/>).

2. Opracowanie wyników

Algorytm batchGCD został wzięty z literatury (<http://facthacks.cr.yp.to/batchgcd.html>) i zaimplementowany w Sage. Jako wejście skrypt przyjmuje plik tekstowy ze sprasowanymi kluczami publicznymi. Prasowanie wykonano dla 9 kluczy publicznych uzyskanych w poprzednim zadaniu za pomocą polecenia „asn1parse” z biblioteki openssl (plik klucze_sparsowane.txt).

```
SageMath version 8.1, Release Date: 2017-12-07
Type "notebook()" for the browser-based notebook interface.
Type "help()" for help.

sage: load("lab.py")
[1, 1, 1, 1, 1, 1, 1, 1, 1]
sage: □
```

Rys 1. Wynik zastosowania algorytmu

Rys. 1 przedstawia wynik zastosowania zaimplementowanego algorytmu batchGCD. Wynik w postaci listy dziewięciu 1., świadczy czy to o braku wspólnych GCD, więc nie udało się odtworzyć private key.

W trakcie wykonania zadania natrafiono na jedną prezentację z konferencji DEF CON 26 (<https://www.youtube.com/watch?v=Z7cLRE6t1Q8&t=4s>), podczas której została przedstawiona strona danej firmy, na której można przetestować klucz publiczny na wrażliwość do GCD i ROCA - <https://keylookup.kudelskisecurity.com>.

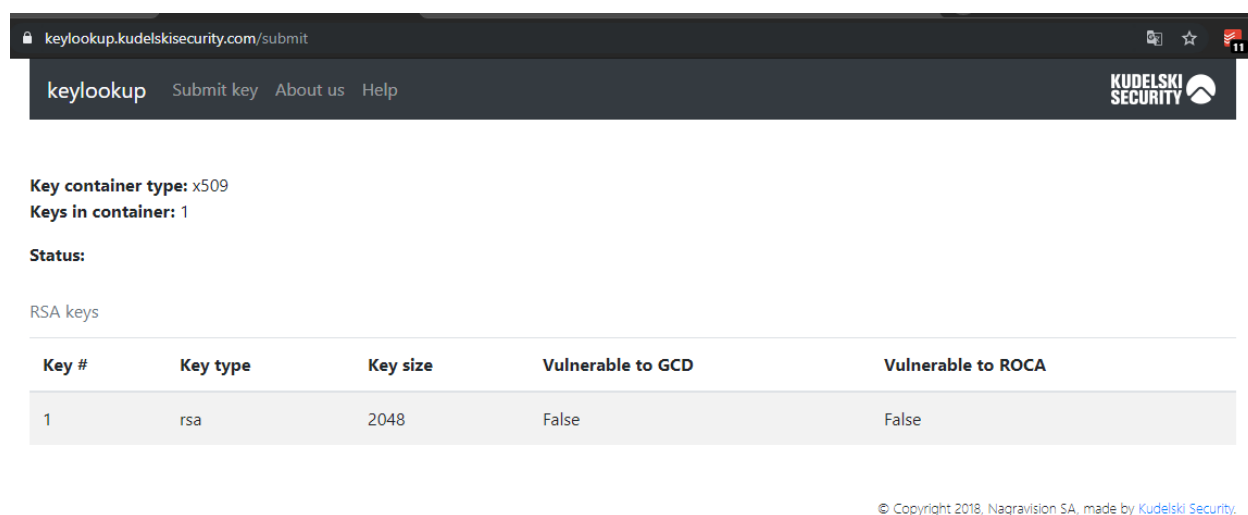
Informacje ze strony: „Zbieramy klucze publiczne RSA z różnych źródeł i analizujemy, czy któryś z tych kluczy ma wspólne czynniki.

Najnowsze wyniki pokazują, że na 1300 jest 1 para kluczy, których bezpieczeństwo jest zagrożone, ponieważ dzieli wspólny czynnik z inną publicznie dostępną parą kluczy.

Nasza baza danych kluczy publicznych zawiera ponad 340 milionów unikalnych modułów RSA. Testowanie nowych kluczy w naszym pełnym zestawie danych zajmuje tylko kilka minut.

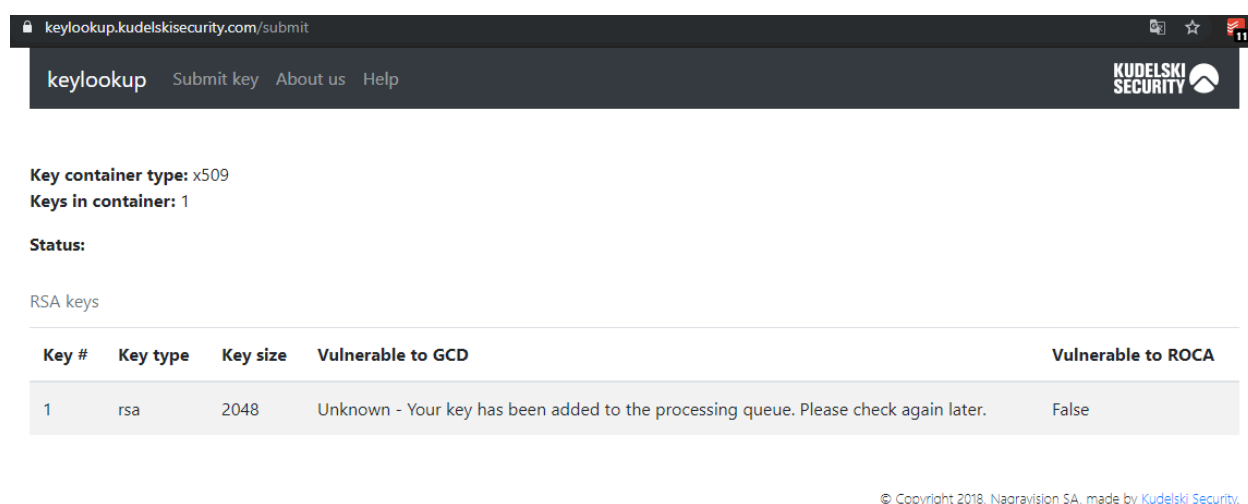
Wrażliwe klucze, które zidentyfikowaliśmy, pochodzą z kluczy SSH gitlab.com, kluczy PGP, certyfikatów stron HTTPS X.509 i innych źródeł.”

W ramach zadania sprawdzono 2 klucze publiczne dla strony www.fizyka.pw.edu.pl oraz www.w3schools.com.



Key #	Key type	Key size	Vulnerable to GCD	Vulnerable to ROCA
1	rsa	2048	False	False

Rys 2. Wynik dla www.w3schools.com



Key #	Key type	Key size	Vulnerable to GCD	Vulnerable to ROCA
1	rsa	2048	Unknown - Your key has been added to the processing queue. Please check again later.	False

Rys 3. Wynik dla www.fizyka.pw.edu.pl

3. Podsumowanie

Zaimplementowano metodę `batchGCD`. Dla wybranych kluczy publicznych nie udało się uzyskać `private key`.