**Na výpočty som použil WolframAlpha.**

**Na výpočet D:**

**http://www.wolframalpha.com/widgets/view.jsp?id=b44389721f078e4ad50fda80d4823ed**

**Úloha číslo 4.**

Úloha č. 4 (RSA algoritmus)

Vypočítajte aspoň 3 privátne kľúče algoritmu RSA a dešifrujte správu (číslo):

1. n = 13169004533; e = 65537; y = 6029832903;
2. n = 1690428486610429; e = 65537; y = 22496913456008;
3. n = 56341958081545199783; e = 65537; y = 17014716723435111315;
4. n = 6120215756887394998931731; e = 65537; y = 5077587957348826939798388;
5. n = 514261067785300163931552303017; e = 65537; y = 357341101854457993054768343508;

Ak sú čísla príliš veľké na faktorizáciu hrubou silou, treba si pomôcť sofistikovaným algoritmom implementovaným v nejakej knižnici alebo napríklad aj Wolfram Alpha.

Úloha 1)

Zadanie:

Nájdem rozdelenie na prvočísla pomocou WolframAlpha:

Hodnota eulerovej funkcie

D:

Dešifrovanie

Úloha 2)

Zadanie:

Nájdem rozdelenie na prvočísla pomocou WolframAlpha:

Hodnota eulerovej funkcie:

D:

Dešifrovanie

Úloha 3)

Zadanie:

Nájdem rozdelenie na prvočísla pomocou WolframAlpha:

Nájdem rozdelenie na prvočísla pomocou WolframAlpha:

Hodnota eulerovej funkcie:

Dešifrovanie:

17014716723435111315^10931906232715055873 (𝑚𝑜𝑑 56341958081545199783) = 1234567890

Úloha 4)

Zadanie:

Nájdem rozdelenie na prvočísla pomocou WolframAlpha:

Nájdem rozdelenie na prvočísla pomocou WolframAlpha:

Hodnota eulerovej funkcie:

Dešifrovanie:

5077587957348826939798388^ 4628379897502241593077665 (𝑚𝑜𝑑 6120215756887394998931731) = 1234567890

Úloha 5)

Zadanie:

Nájdem rozdelenie na prvočísla pomocou WolframAlpha:

Nájdem rozdelenie na prvočísla pomocou WolframAlpha:

Hodnota eulerovej funkcie:

Dešifrovanie:

357341101854457993054768343508^ 138834873007999909396179588113 (𝑚𝑜𝑑 514261067785300163931552303017) = 1234567890