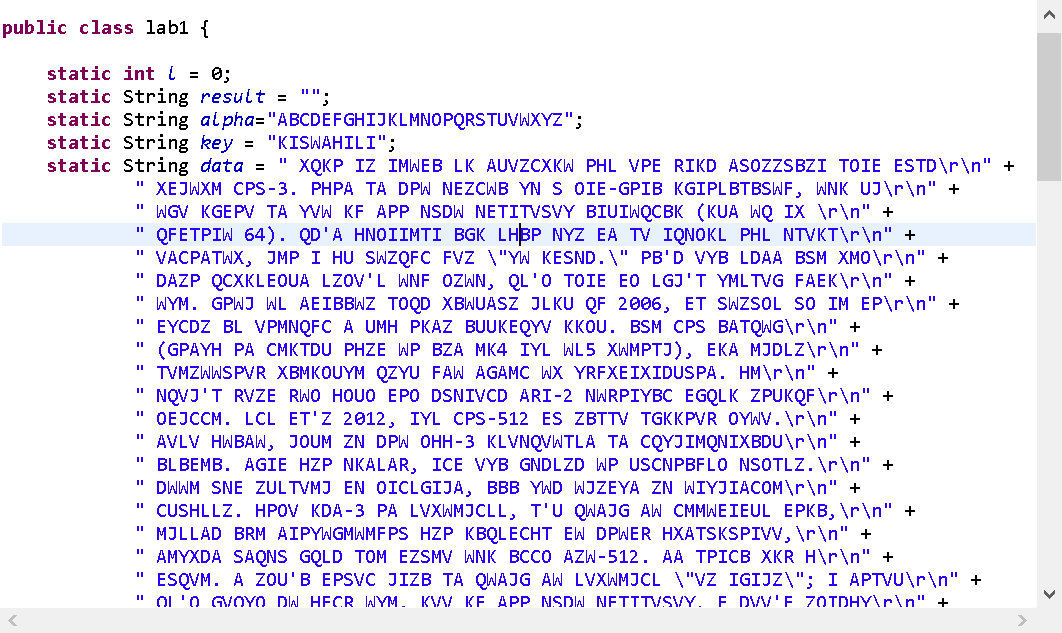
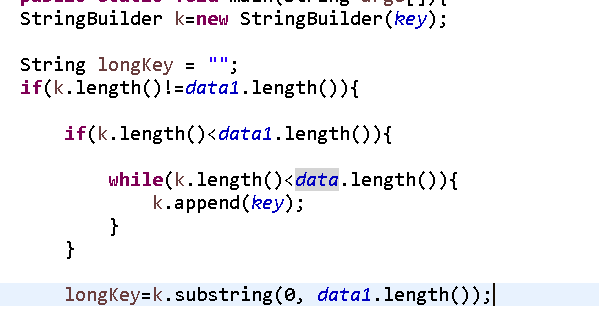
Vigenere

Reference: https://en.wikipedia.org/wiki/Vigen%C3%A8re\_cipher

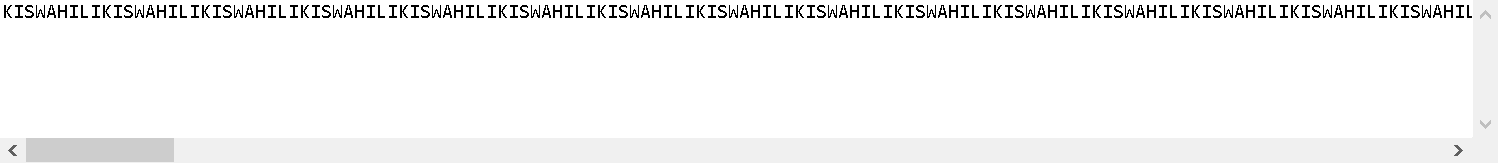




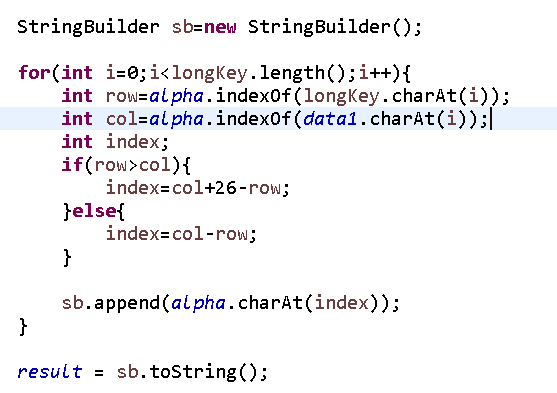
First initialize variable for key, alpha and ciphertext, and delete all symbol.



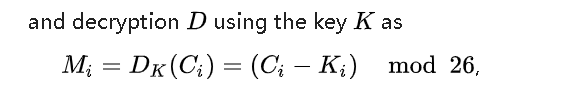
Make key longer, cut it same length with ciphertext without symbol. Make key and ciphertext as table. The column of table is ciphertext and row of table is key.



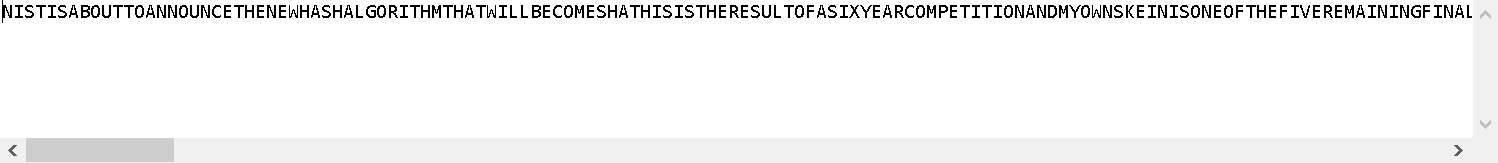
output longKey.



Find location of `letter of key and ciphertext in alpha.

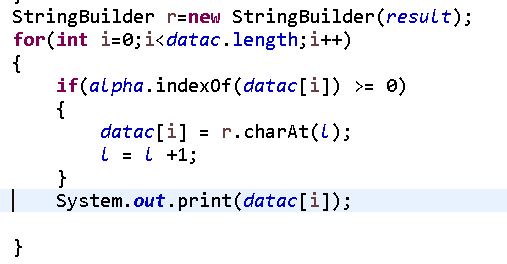


Use this formula to find location of letter of plaintext in alpha.

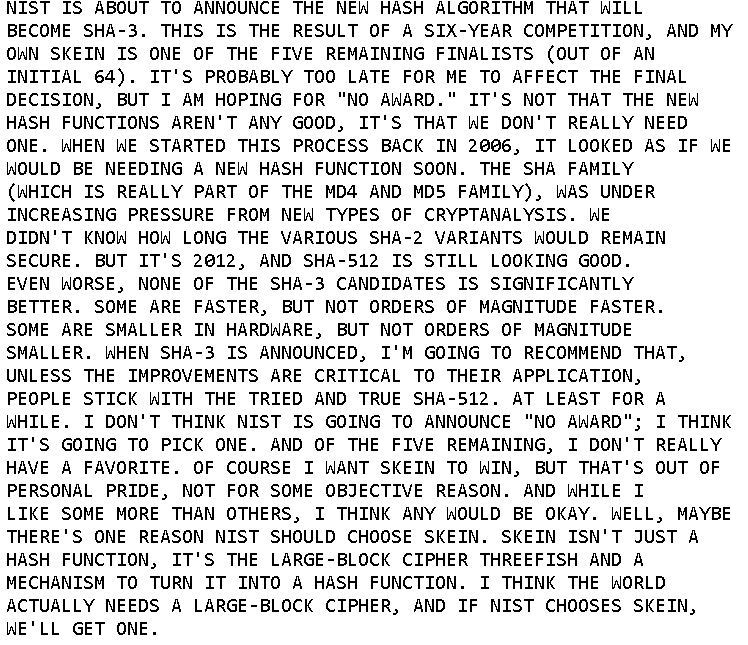


Output result. But the result is without symbol.





Replace all letters from ciphertext to plaintext, this will keep all symbol. The final result is in the below.



RSA

BigInteger introduct and formula ref: <http://www.ruanyifeng.com/blog/2013/07/rsa_algorithm_part_two.html>

BigInteger Multiply Ref：<http://java2s.com/Tutorials/Java/BigDecimal_BigInteger/How_to_add_subtract_multiply_and_divide_a_Java_BigInteger.htm>

BigInterger subtract ref:

<https://stackoverflow.com/questions/15902789/biginteger-in-java>

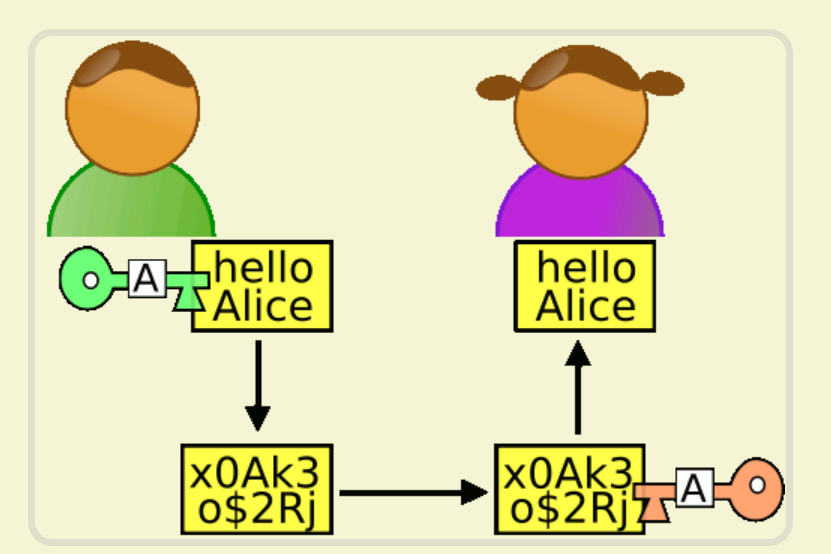
prime ref: <https://www.tutorialspoint.com/java/math/biginteger_probableprime.htm>

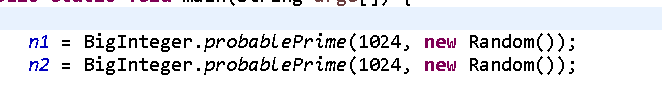
Big Integer compare ref: <https://www.geeksforgeeks.org/biginteger-compareto-method-in-java/>

Euclid’s extended algorithm ref: <https://www.tutorialspoint.com/java/math/biginteger_modinverse.htm>

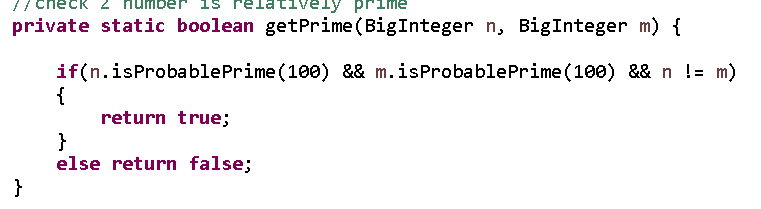
Modpow ref: <https://www.javatpoint.com/java-biginteger-modpow-method>

String and big integer exchange: <https://stackoverflow.com/questions/50497085/how-can-i-convert-a-biginteger-string-to-an-ascii-string>

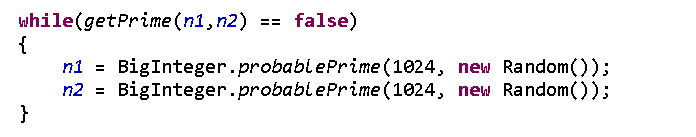




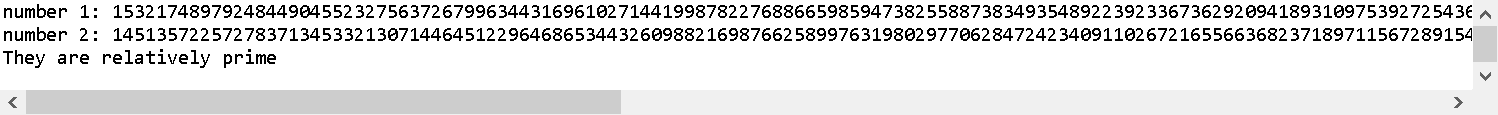
First create 2 big integer and set length is 1024.

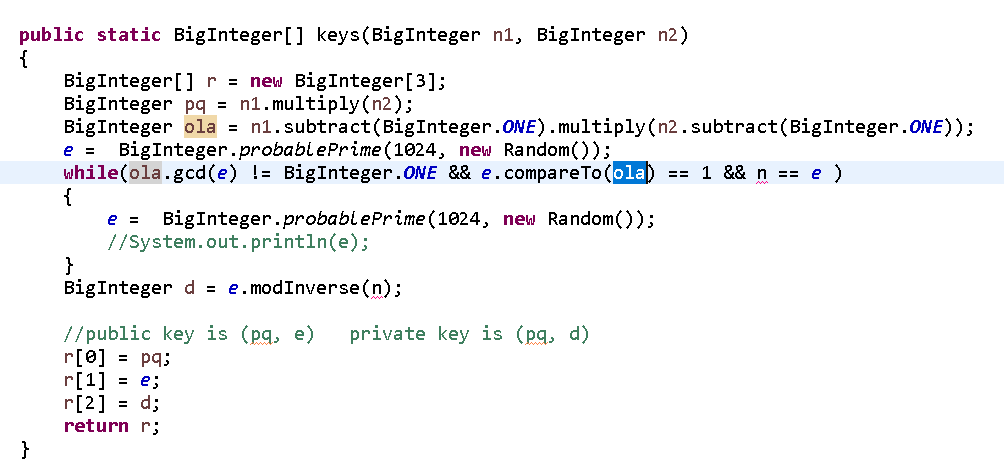


Check 2 big integer is relative prime, if number 1 is prime, number 2 is prime and they are not same, so they are relative prime.



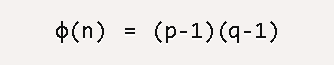
If they not relative prime will use while loop to create new number to make sure they are relative prime. Result as below.

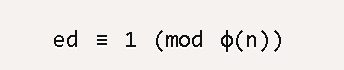


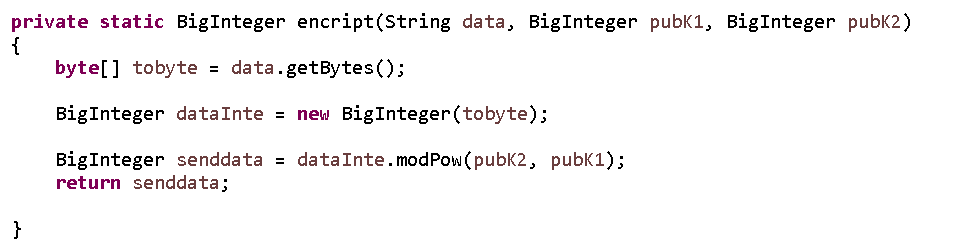


Find public key (pq, e) and private key (pq, d) use below formula. Pq is n of below, ola is φ(n) of below, e is random pick from 1 to ola and e is relative prime with ola, d is ed of below.

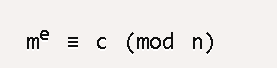


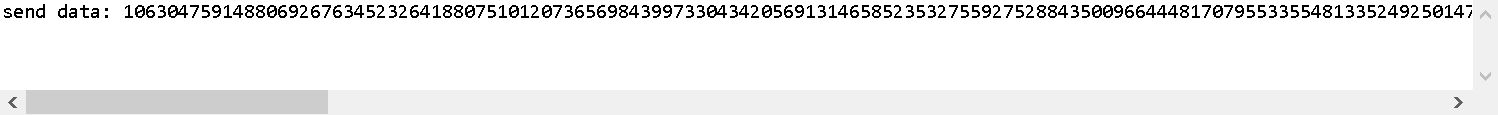


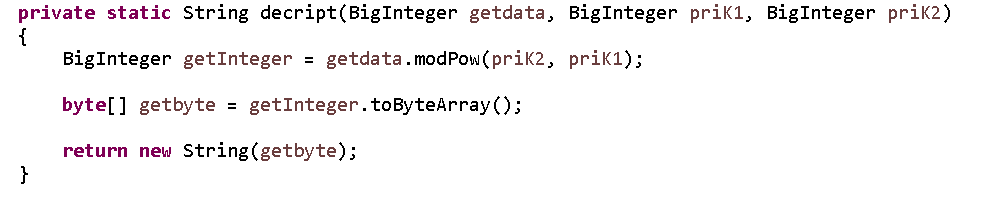




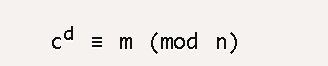
Change data to big integer then use public key follow formula of below to encryption. dataInte is m of below, senddata is c of below, pubK2 is e of below and pubK1 is n of below.

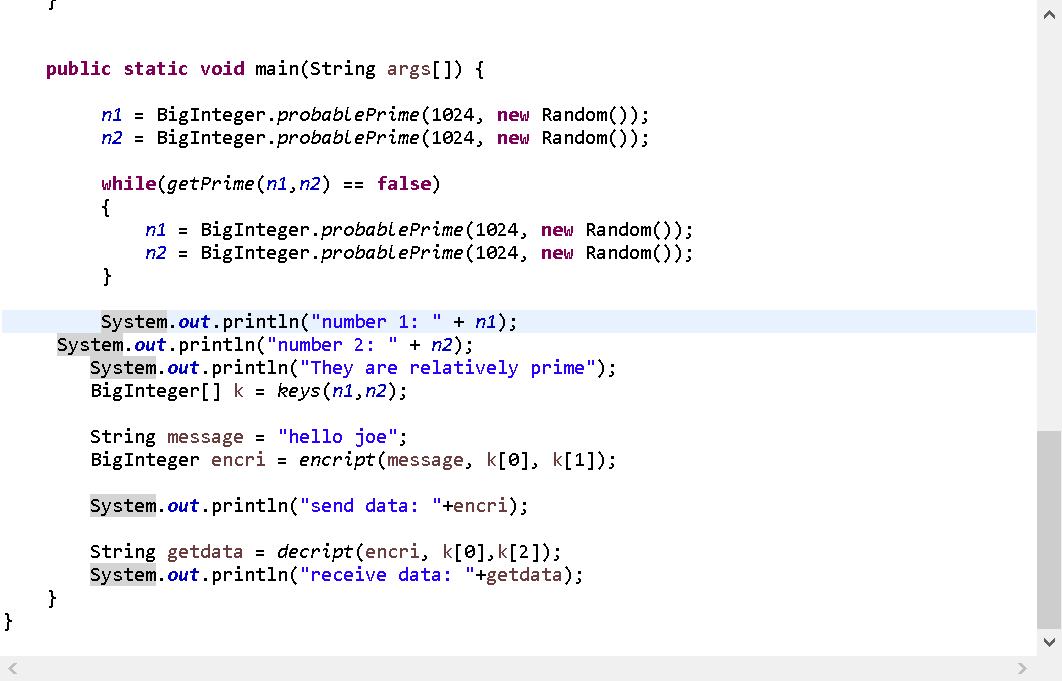




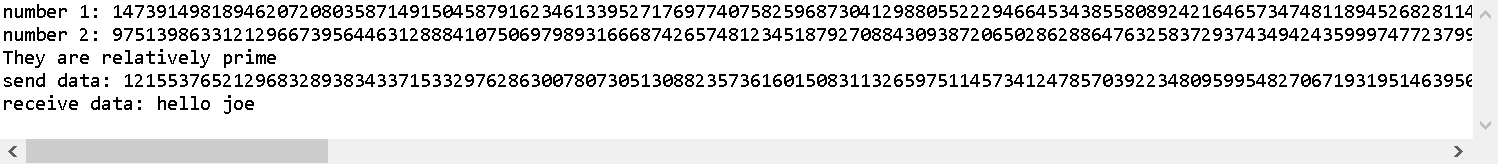


Use private key follow formula of below to decryption, then change big integer to string.

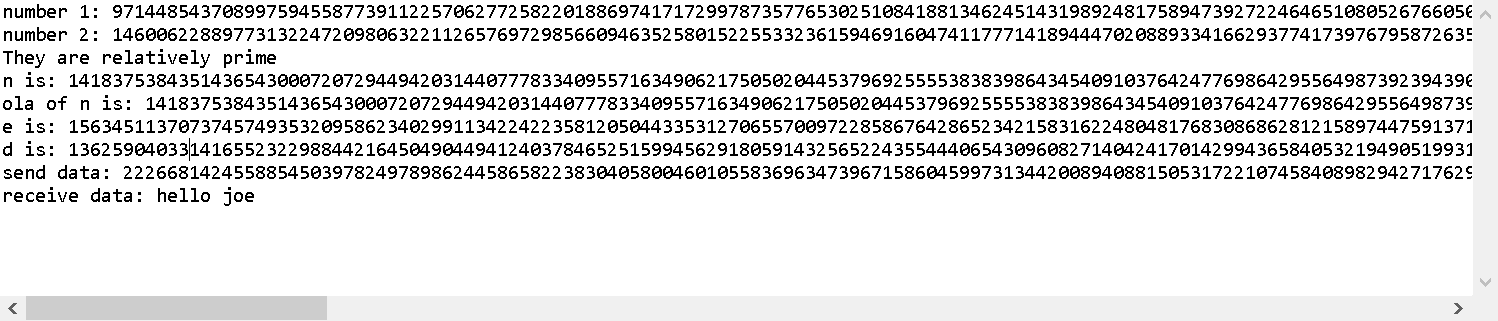


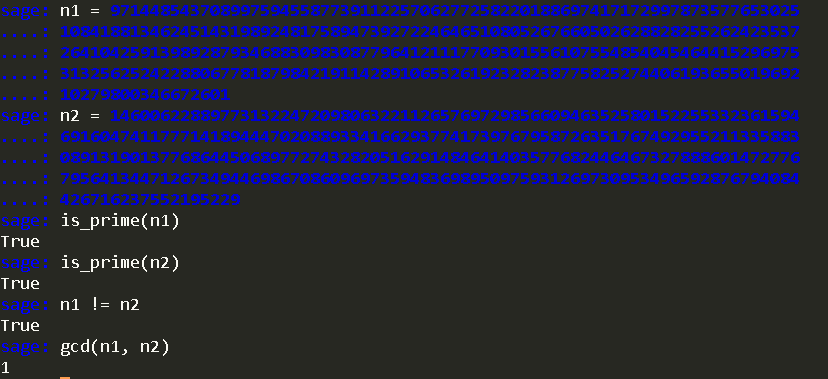


Implement method in the main. Result as below

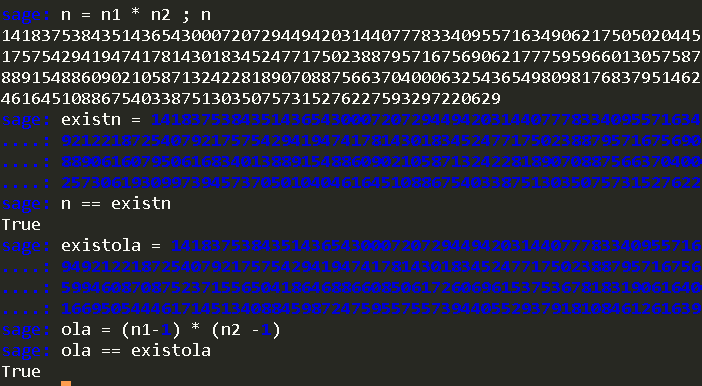


Cryptographic Tools

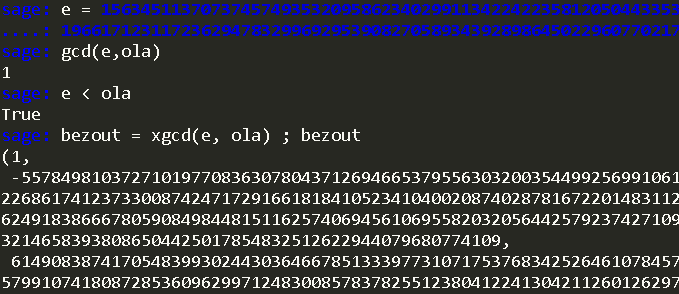


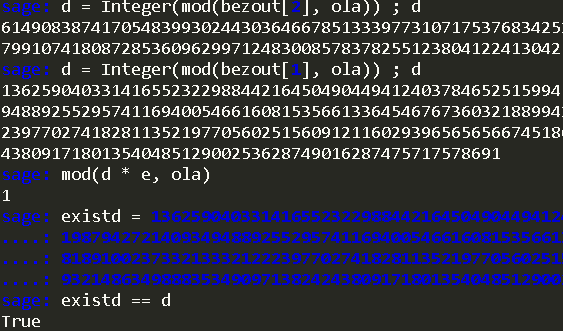


Check 2 random number is prime and not same, so they are relative prime

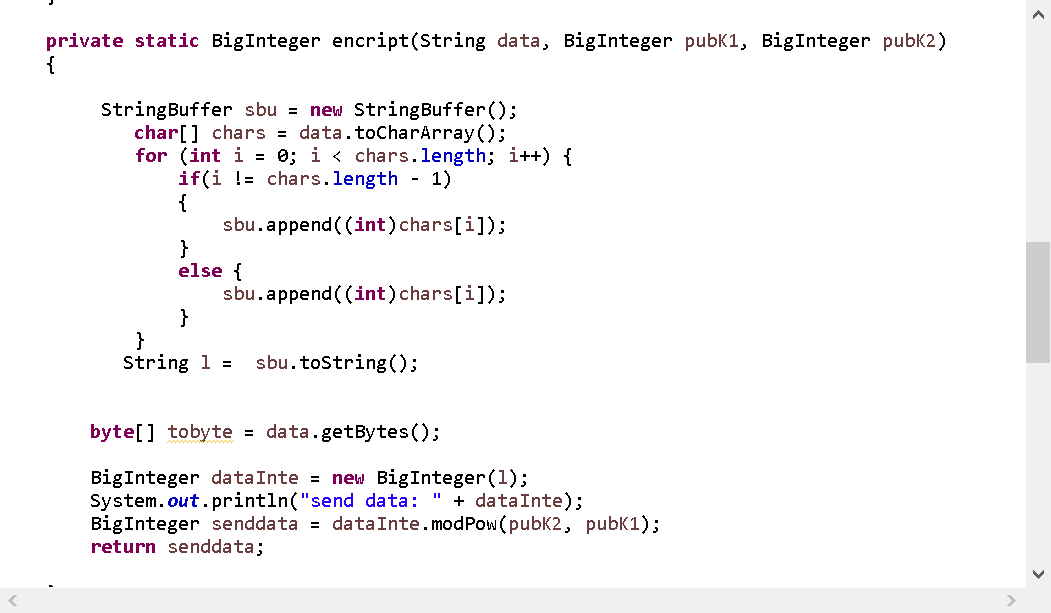


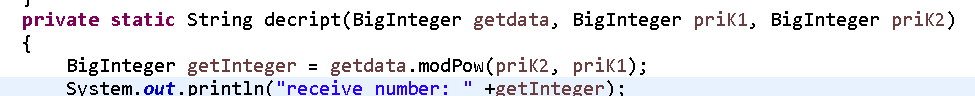
Check n is and euler of n same with coding.



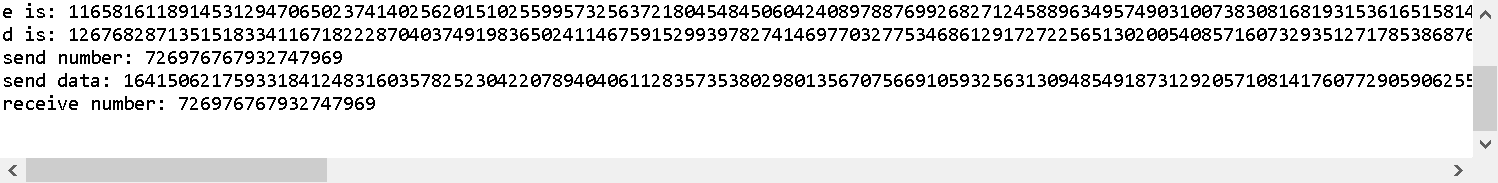


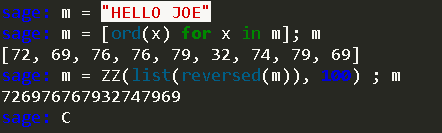
Check e is relative prime with euler of n, e less than euler of n. check d is same with coding.



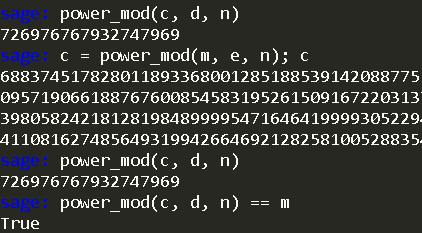


Add string to integer in encrypt.



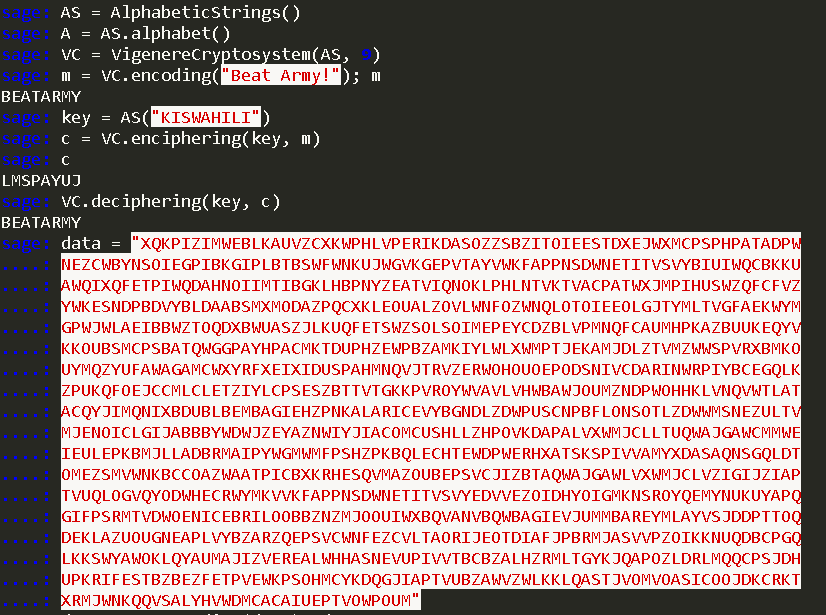


Change string to integer.



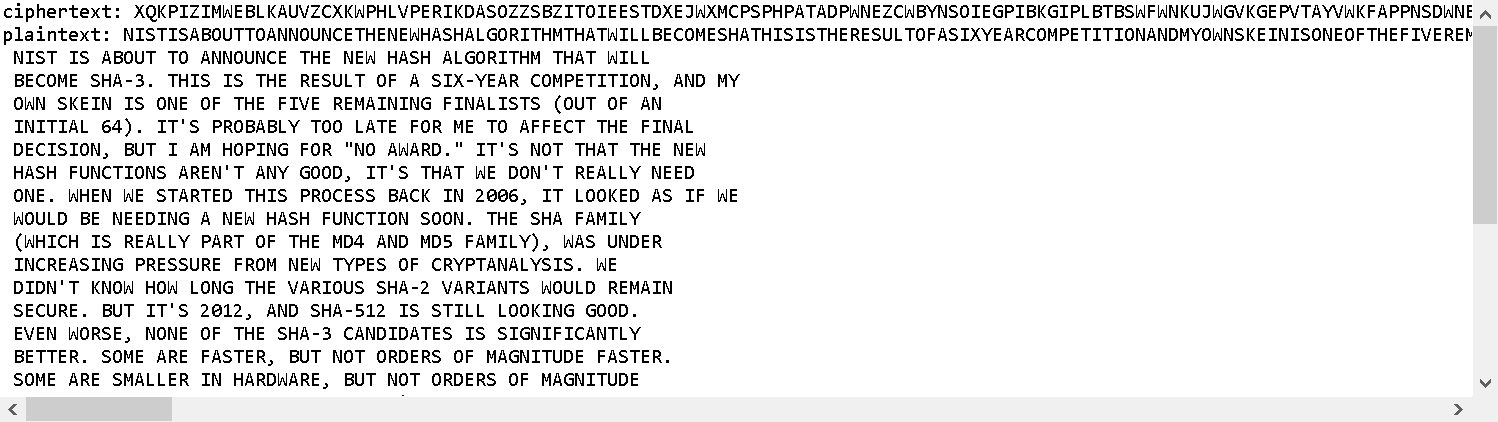
Encrypt and decrypt for integer, is same and same with coding as well.

Vigenere





Use sage to decrypt ciphertext for vigenere cipher find reults. Then compare with coding is some.



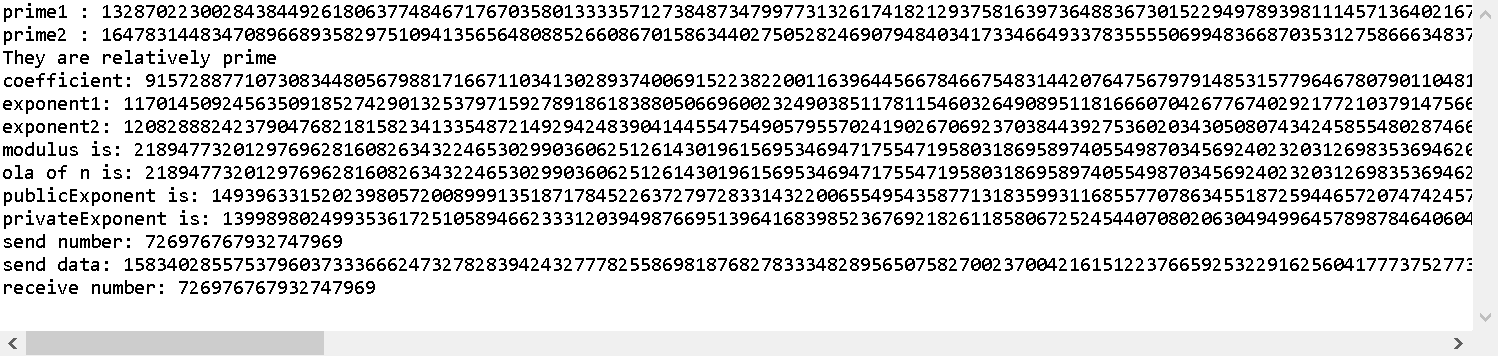
Openssal

Reference:

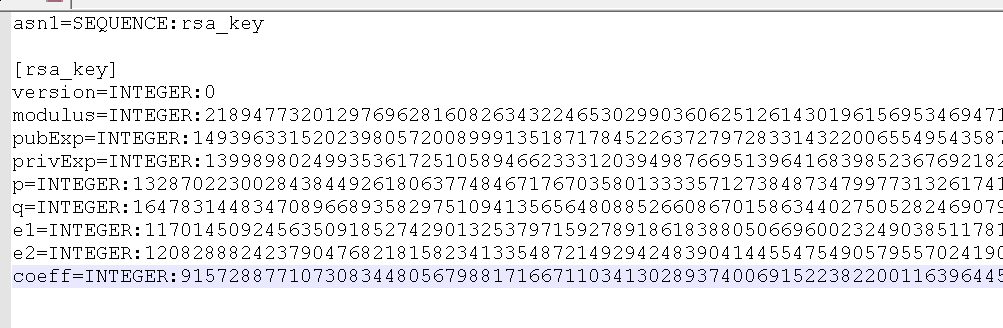
<https://my.oschina.net/fenying/blog/786238>

<http://fileformats.archiveteam.org/wiki/DER_encoded_RSA_private_key>

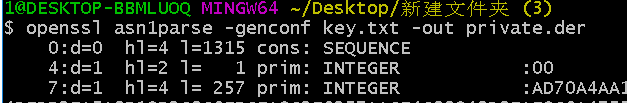
<https://stackoverflow.com/questions/19850283/how-to-generate-rsa-keys-using-specific-input-numbers-in-openssl>



Use java to print out p, q, n, e, d ect.



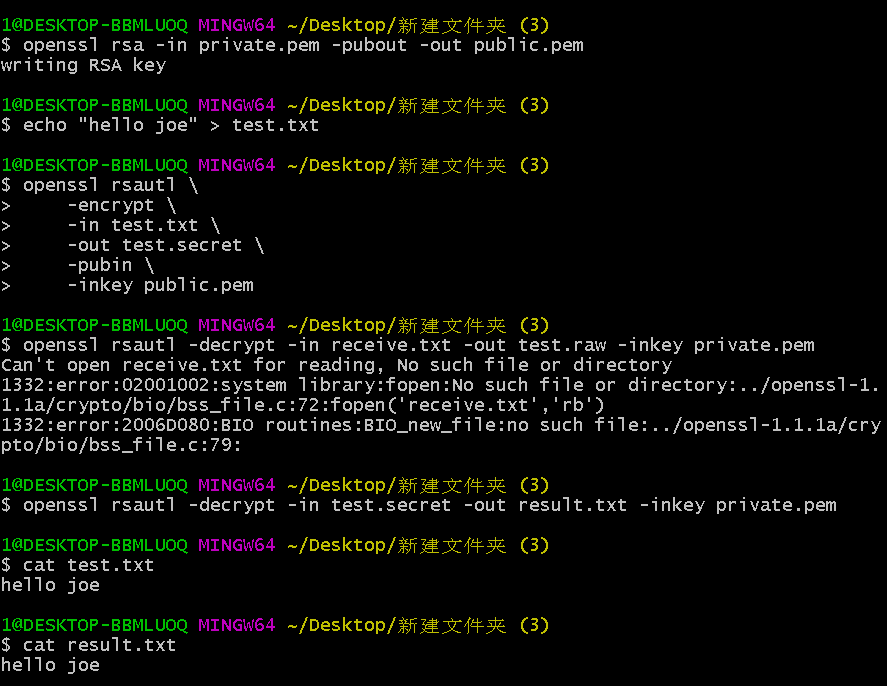
Write those argument in text file.



Change text file to der file.



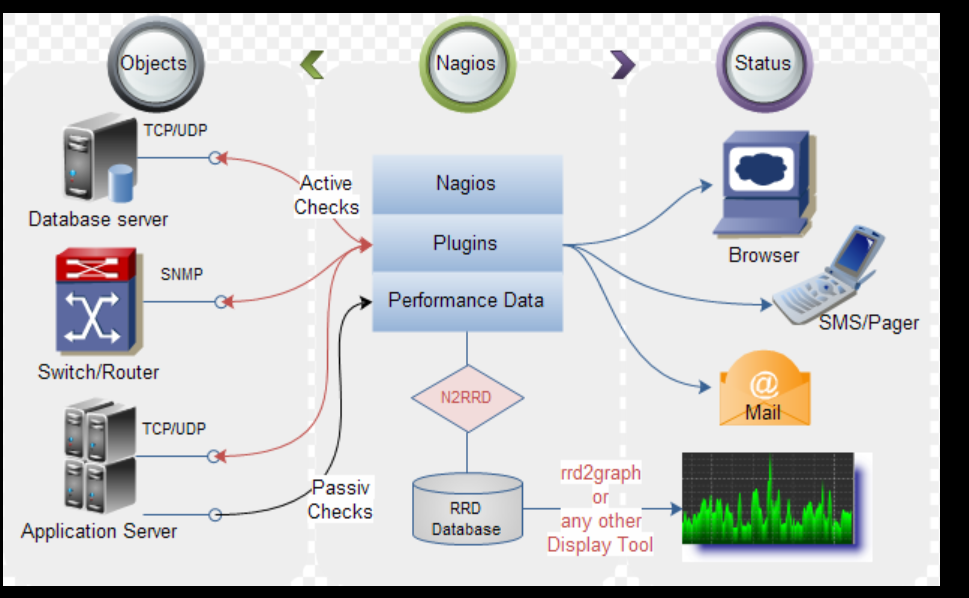
Change primary key der file to pem file. And check as private key.



Create public key from private key, then create a test txt file as transform data, use public key to encrypt data, use private key to decrypt data print out result txt is same with test txt. That I can testimonial primary key from eclipse is useful.



**Security Monitoring and Vulnerability**



Nagios is open source application use to Monitoring systems and networks. Then client program is deployed on the server to be monitored. That allowed server and client communication to monitoring different source of client.

Nagios can monitor most project.

if Nagios detect Anomaly happens will sent web page to your mobile or email, that you can through open web page to check anomaly of source.

Advantages:

* Increased server, services, process, and application availability
* Fast detection of network and server outages and protocol failures
* Fast detection of failed servers, services, processes and batch jobs

**Ten vulnerabilities**

1. Microsoft Windows HTTP.sys Code Execution Vulnerability

Web server

HTTP.sys in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold and R2 allows remote attackers to execute arbitrary code via crafted HTTP requests, aka "HTTP.sys Remote Code Execution Vulnerability."

Successful exploitation will allow remote attackers to cause a buffer overflow and potentially execute arbitrary code with SYSTEM privileges

1. Windows Terminal Service Detection

Backdoors

The Terminal Services are enabled on the remote host. Terminal Services allow a Windows user to remotely obtain a graphical login and therefore act as a local user on the remote host.

If an attacker gains a valid login and password, he may be able to use this service to gain further access on the remote host.

1. Microsoft's SQL TCP/IP Listener

The remote host is running MSSQL, a database server from Microsoft. It is possible to extract the version number of the remote installation from the server pre-login response.

Attackers can gain critical information about the host.

1. Internet Explorer 8 Allows Code Execution (KB2847140)

|  |  |
| --- | --- |
| Category: | Policy Checks |

as exploited in the wild in May 2013. The remote version of IE reportedly has a use-after-free flaw related to how CGenericElement objects are handled that could result in arbitrary code execution on the remote system.

vulnerability in Internet Explorer 8 Could Allow Remote Code Execution

1. **Insecure Library Loading Allows Code Execution (KB2269637)**

|  |  |
| --- | --- |
| Category: | Policy Checks |

working directory when resolving DLL dependencies. If a malicious DLL with the same name as a required DLL is located in the application's current working directory, the malicious DLL will be loaded.

A remote attacker could exploit this issue by tricking a user into accessing a vulnerable application via a network share or WebDAV folder where a malicious DLL resides, resulting in arbitrary code execution.

1. PHP Running Version Prior to 5.2.15

|  |  |
| --- | --- |
| Category: | Server Side Scripts |

in PHP 5.3.x through 5.3.3 might allow remote attackers to bypass open\_basedir restrictions via vectors related to the length of a filename. \* Double free vulnerability in the imap\_do\_open function in the IMAP extension (ext/imap/php\_imap.c) in PHP 5.2 before 5.2.15 and 5.3 before 5.3.4 allows attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via unspecified vectors.

1. **Vulnerabilities in Unauthorized Digital Certificates Allow Spoofing (KB2728973)**

Category: Policy Checks  
The remote host is missing Microsoft KB2264107, The remote host is missing KB2728973, which updates the system's SSL certificate blacklist.

Unauthorized digital certificates could allow spoofing, phishing, or man in the middle attacks.

1. **Vulnerabilities in Server Service Allows Code Execution (MS08-067, Network)**

|  |  |
| --- | --- |
| Category: | SMB/NetBIOS |

The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary code via a crafted RPC request, as exploited in the wild in October 2008, aka Server Service Vulnerability.

An attacker who successfully exploited this vulnerability could take complete control of an affected system remotely.

1. **PHP Unsupported Version Detection**

|  |  |
| --- | --- |
| Category: | Server Side Scripts |

According to its version, the installation of PHP on the remote host is no longer supported. As a result, it is likely to contain security vulnerabilities.

Anyone can connect to the NSClient and retrieve sensitive information, such as process and service states, memory usage, etc.

1. **NSClient Default Password**

|  |  |
| --- | --- |
| Category: | Simple Network services |

The remote host is running an instance of NSClient, an addon for Nagios used to monitor Windows hosts, configured using a default password.

Anyone can connect to the NSClient and retrieve sensitive information, such as process and service states, memory usage, etc.

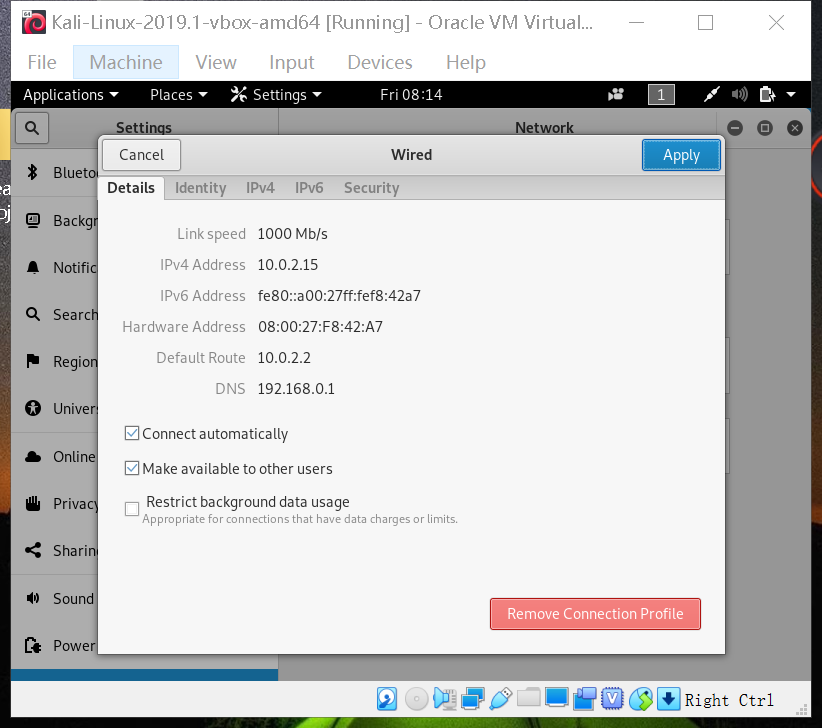
<https://en.wikipedia.org/wiki/Nagios>

<https://www.nagios.com/solutions/server-monitoring/>

<https://www.beyondsecurity.com/top_network_web_application_vulnerabilities.html>

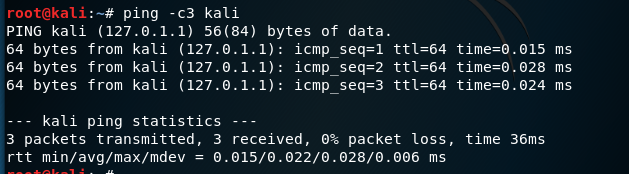
Kali Linux

* 1. What's your computer's IP address for its current Internet connection? (How can you tell the difference between your Ethernet IP and your wireless IP if you have both connections active?)

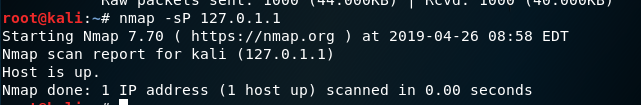




* 1. How can you determine the IP address associated with a given host name?



* 1. How can you determine the host name(s) associated with a given IP address?



Ref: <https://www.linuxquestions.org/questions/linux-newbie-8/basic-command-to-resolve-ip-to-hostname-582026/>

4. How can you copy a file from one computer to another? Or more to the point, if you create a file on the Kali virtual machine and you want to put it someplace where you can save it, how do you go about it from the Kali command-line interface?

5. How can you tell whether there's a process listening on a given port (e.g. port 80 or port 22) on a given host?

6. How can you tell which ports have processes listening on them on a given host?

7. How can you retrieve and save a given web page (say http://google.com/ in a file on your system?

8. How can you view the HTTP headers sent back from a specified web server when you request one of its pages?

9. [Super bonus question] Is there a command-line-only way to view the HTTP headers that \*my\* computer sends when I run the commands in the previous two questions?