

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/328630416>

Analysis of asymmetric cryptography in information security based on computational study to ensure confidentiality during information exchange

Research · October 2018

DOI: 10.13140/RG.2.2.30495.61602

CITATION

1

READS

2,674

3 authors, including:



Abdul Ghaffar Khan

University of Management and Technology (Pakistan)

7 PUBLICATIONS 32 CITATIONS

[SEE PROFILE](#)



Muhammad Usama Riaz

University of Management and Technology (Pakistan)

5 PUBLICATIONS 28 CITATIONS

[SEE PROFILE](#)

Some of the authors of this publication are also working on these related projects:



Prediction of Heart Disease using Artificial Neural Network [View project](#)



PREDICTION OF HEART DISEASE USING ARTIFICIAL NEURAL NETWORK [View project](#)

Analysis of asymmetric cryptography in information security based on computational study to ensure confidentiality during information exchange

Abdul Ghaffar Khan, Sana Basharat, Muhammad Usama Riaz

Abstract— Asymmetric cryptography is a cryptographic system in which public and private keys are used as a pair. Public key is dispersed publicly and the other side private key known by owner only. Public key is very efficient for authentication as well as for encryption. Public key for encrypt (conversion from data or information to code) and private key for decrypt (reciprocal of encryption or reverse process of encryption) a message. Nowadays it is very difficult to decide the key length to use for proper information security. The long length of the keys takes huge time, but more security. In this article, we propose that to explore authentication and confidentiality of information during transportation by implementing the RSA algorithm. Rivest-Shamir-Adleman (RSA) algorithm is widely used in asymmetric (public key) cryptography for encryption and decryption of information.

Index Terms— Asymmetric Cryptography, authentication, Cryptography, Confidentiality, Information security, RSA algorithm.

1 INTRODUCTION

Asymmetric key is also known as a public key. Key pairs (public, private) are used in asymmetric cryptography where public key is distributed publicly and private key is used on the decryption side to convert the cipher text into plain text. Highly used of the asymmetric key is to secure exchange of communication on the internet. For encryption of asymmetric key, we use the RSA algorithm for better and secure transaction on the internet. Asymmetric is a little bit slower rather than symmetric due to computations on cryptography of asymmetric key. SSL is the well-known example where the asymmetric key is used for safe and secure communication on the internet. In this article, we propose that how to maintain authentication and confidentiality of information during transportation by implementing the RSA algorithm, where it will ensure confidentiality of information. RSA algorithm is widely used in asymmetric cryptography for encryption and decryption of information. Remember that confidentiality means protection of message from observer and authentication means that the receiver needs assurance as the identity of the sender.

2 RELATED WORK

In this paper [1] they highlighted the RSA's computational complexity, encryption and authentication of asymmetric. In symmetric cryptosystems, the sender and receiver key are either the same or easy to compute them. But the other hand, where we cannot have the same case like symmetric, we have three possible ways. 1) Forward asymmetric: Here private key is very difficult to be computed given sender's key. 2) Backward asymmetric: At this point public key is very tough to be computed given receiver's key. 3) Bidirectional asymmetric: Both public and private keys cannot be computed given the other. Bidirectional encryption has two characteristics. 1) Secure communication is possible. Even sender's key has been compromised during communication. Its

use in forward asymmetric encryption. 2) Sender's message authentication is possible, even if receiver's key is compromised. It is used in the backward encryption system. Factorization trapdoor is a public key encryption concept RSA. It can find prime numbers in time $O(d^3)$, if we take large number (n) then its complexity of factoring exceeds from any polynomial limit. Now $O(n(\ln n)/\ln n)^{1/2}$. In suggested system p and q are pairs of primes so $n=pq$ is away from all expected computational capabilities. Pairs of e and d where $(e, \phi(n)) = 1$ and $ed \equiv 1 \pmod{\phi(n)}$; $\phi(n) = (p-1)(q-1)$. Here e and d are the multiplicative inverse of remains classes modulo $\phi(n)$. When we start cryptosystem as public keys, e and n goes in public key list and d is set aside secret. The receiver knows p and q , the system is forward asymmetric.

In paper [2] they focus on cryptography techniques as they mention in conclusion that a cryptographic scheme that comprises symmetric and asymmetric algorithms is projected for securing safe data transmission via satellite-based communication channel. Java programming is used to develop software based on this scheme. Results show that, by utilizing information confidentiality, integrity and information authentication, which are the essential features for information security in satellite-based communication. They discussed confidentiality, integrity; authentication and identification are the key properties of proposed scheme. In authentication and identification by using a hashing algorithm with a combination of asymmetric algorithm and it gives the digital signature which provides assurance for validity of origin of the information. IDEA (utilize 128 bit key), RSA (1024 bit key) and MD5 (128 bits hash) algorithms are used for secured communication.

Here [3] they have seen a complete analysis of the asymmetric key algorithms. Author of this paper publicize a picture of their encryption and decryption procedures to categorize their current gap grounded on ending drawn from the analysis, with certain weight on an algorithm utmost well-matched for industrial ap-

publication specified the current inclinations in cryptography in the direction of quantum computing. The earnest necessity for an algorithm that has nearly no trade-off in encryption and decryption work action speed has low computation above and is protected sufficient to resist quantum algorithm attacks. In this paper author totally target on the public key cryptography algorithms. It is very important to notice that private key algorithms almost so far faster as I have said that 2 to 3 orders of degree faster than public key methods or algorithms. However, public key algorithms offer extra higher security and have extensive enactment. Author tried to provides a in order understanding for the development of different keys especially public key algorithms. According to a performance evaluation conducted in 2000, in comparison to RSA1024 and ECC168 (Ecdh), NTRU had the fastest encryption, decryption and key generation speed. NTRUs speed was approximately two orders of magnitude more rapidly than ECC (in a CPU). However, NTRU had the largest public key size and the message expansion is twice as much as that of ECC at an equivalent security level.

In this paper [4], author given a sketch on implementation of cryptography and briefly discussed on symmetric and asymmetric cryptography. Embedded hardware and software were target of author where to implement cryptosystem. They tell the difference or distinguish symmetric and asymmetric ciphers, because the latter offers more security functionality and therefore have different application scenarios. Symmetric ciphers serve primarily used for text or string which sent to check its integrity, secondly it used for entity authentication, thirdly and at the last is used to check encryption.

In this paper [5] they have discussed literature reviews the daily used algorithms, in consort with the anticipated algorithms based on their positivity and negativity, associated to Symmetric and Asymmetric Key Cryptography. They have also likened the value of mutually these techniques. The anticipated algorithms showed to be cryptographic extremely well-organized in their particular grounds but there is a related part that persisted open, interrelated to these algorithms, and have still not been thoroughly discussed. This paper [5] also presents an appropriate future scope associated to these open fields. They have highlighted the basic as well as proposed algorithms related to these cryptographic (encryption and decryption) methods. The public key will remain open or public and the private keys not shared. This technique ensures better security than the former. Furthermore, the main part which make data highly confidential and non-repudiation is the use of digital signature.

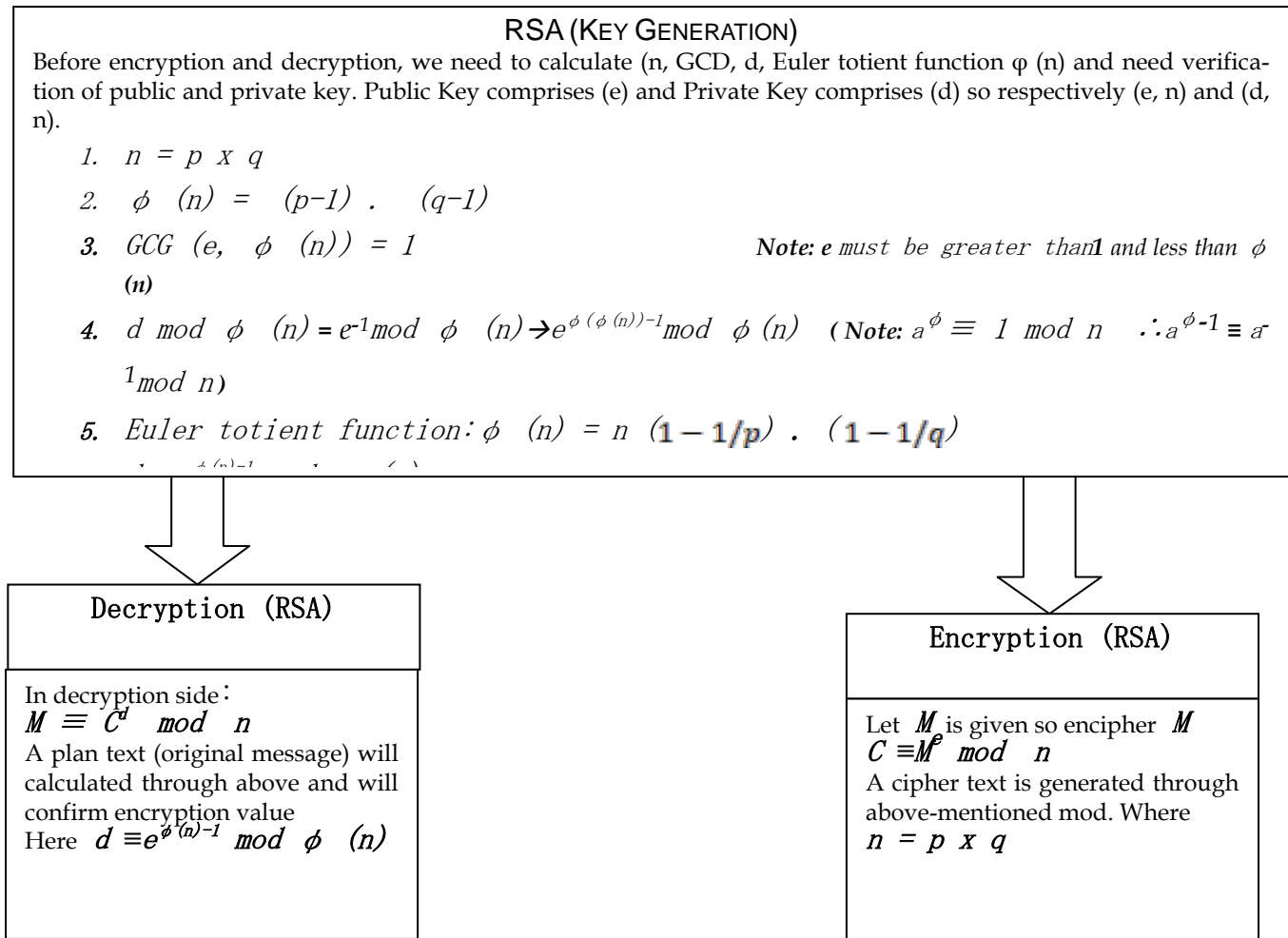
3 PROBLEM STATEMENT

In this cryptographic scenario, it is very hard to achieve authentication and confidentiality with integrity just in a single step. In public key encryption and decryption carry out with a dissimilar key, but where symmetric key will not be as like shareable entity. As like asymmetric key cryptography where we use symmetric key for encryption of message, but using its public key anyone can decrypt the message. When we attempt to achieve authentication, then it is difficult to maintain confidentiality. When we use a public key for the purpose to encrypt the message, only anticipated receiver can decrypt the message. Here we managed confidentiality, but simultaneously we cannot

maintain authorize the sender. Now we need to overcome the above-mentioned problem. For this, after private key we use public key encryption. After that, only anticipated recipient would be capable to decrypt the message and simultaneously he will also be capable to check the authenticity sender by decrypting cipher message using public key.

4 RSA ALGORITHM FOR AUTHENTICATION AND CONFIDENTIALITY

RSA implementation form initialization of a message from encryption side to decryption of a message is given below, for general sketch about RSA implementation and their corresponding steps. Confidentiality and proper confirmation of message is given in below example.



4.1 IMPLEMENTATION OF RSA ALGORITHMS

i. Key Generation

First of all we need to generate two distinct but random prime numbers like p and q.

Let suppose p= 11, q= 5 so

$$n = p \times q \rightarrow (11) \cdot (5) = 55$$

So key length is 55

$$\phi(n) = (p-1) \cdot (q-1) \rightarrow (11-1) \cdot (5-1)$$

$$\phi(n) = 40$$

$$e = 3$$

Note: e must be greater than 1 and less than $\phi(n)$

GCD calculation through Euclidean Algorithm

$$40 = 3(13) + 1$$

$$3 = 1(3) + 0$$

$$\text{So } (3, 40) = 1$$

$$\text{Here } GCD(e, \phi(n)) = 1,$$

Calculation of d by following steps number 4 to onward from (**Error! Reference source not found.**) declaration as we know that

$$d.e \equiv 1 \pmod{\phi(n)}$$

$$d \pmod{\phi(n)} = e^{-1} \pmod{\phi(n)} \rightarrow e^{\phi(\phi(n))^{-1}} \pmod{\phi(n)}$$

(Note: $a\phi \equiv 1 \pmod{n} \therefore a^{\phi-1} \equiv a^{-1} \pmod{n}$)

$$d \pmod{\phi(n)} = e^{\phi(n)-1} \pmod{\phi(n)}$$

$$d \pmod{\phi(n)} = e^{40-1} \pmod{40}$$

$$d \pmod{\phi(n)} = e^{39} \pmod{40}$$

→ Euler totient function ←

$$\phi(n) = n \left(1 - \frac{1}{p}\right) \cdot \left(1 - \frac{1}{q}\right)$$

$$\phi(40) = 40(1-1/2) \cdot (1-1/5)$$

$$\phi(40) = 16$$

$$\text{Now } d \equiv e^{\phi(n)-1} \pmod{\phi(n)}$$

$$d \equiv e^{16-1} \pmod{40}$$

$$d \equiv e^{15} \pmod{40}$$

$$d \equiv e^{8+4+2+1} \pmod{40}$$

$$d \equiv e^8 \cdot e^4 \cdot e^2 \cdot e^1 \pmod{40}$$

$$d \equiv 1^8 \cdot 1^4 \cdot 3^2 \cdot 3^1 \pmod{40}$$

$$d \equiv 1 \cdot 1 \cdot 9 \cdot 3 \pmod{40}$$

$$d \equiv 27 \pmod{40}$$

→ Verification ←

Public Key (e, n)

Private Key (d, n)

We know that

$$d.e \equiv 1 \pmod{\phi(n)}$$

so,

$$(27 \cdot 3) \equiv 1 \pmod{40}$$

$$81 \equiv 1 \pmod{40}$$

It satisfies the relation

$$d.e \pmod{\phi(n)} = 1$$

ii. Encryption

Let M = 8,

$$C \equiv M e \pmod{n}$$

$$C \equiv 83 \pmod{55}$$

$$C \equiv 82+1 \pmod{55}$$

$$C \equiv 82.81 \pmod{55}$$

$$C \equiv 9.8 \pmod{55}$$

$$C \equiv 72 \pmod{55}$$

$$C \equiv 17 \pmod{55}$$

Decryption

$$M \equiv C d \pmod{n}$$

$$M \equiv 1727 \pmod{55}$$

$$M \equiv 1716+8+2+1 \pmod{55}$$

$$M \equiv 1716.178.172.171 \pmod{55}$$

$$M \equiv 16.26.14.17 \pmod{55}$$

$$M \equiv 99008 \pmod{55}$$

$$M \equiv 8 \pmod{55}$$

Here decryption successfully done.

4.2 CONFIDENTIALITY AND AUTHENTICATION

In introduction as we discussed that confidentiality mean protection of message from observer and authentication mean that receiver needs assurance as the identity of sender. In following figure 1; PUA and PRA are respectively designated as public and private keys, same like above PUB and PRB are respectively designated as public and private keys. In figure 1; A wants to send a message to B by maintaining confidentiality and authentication.

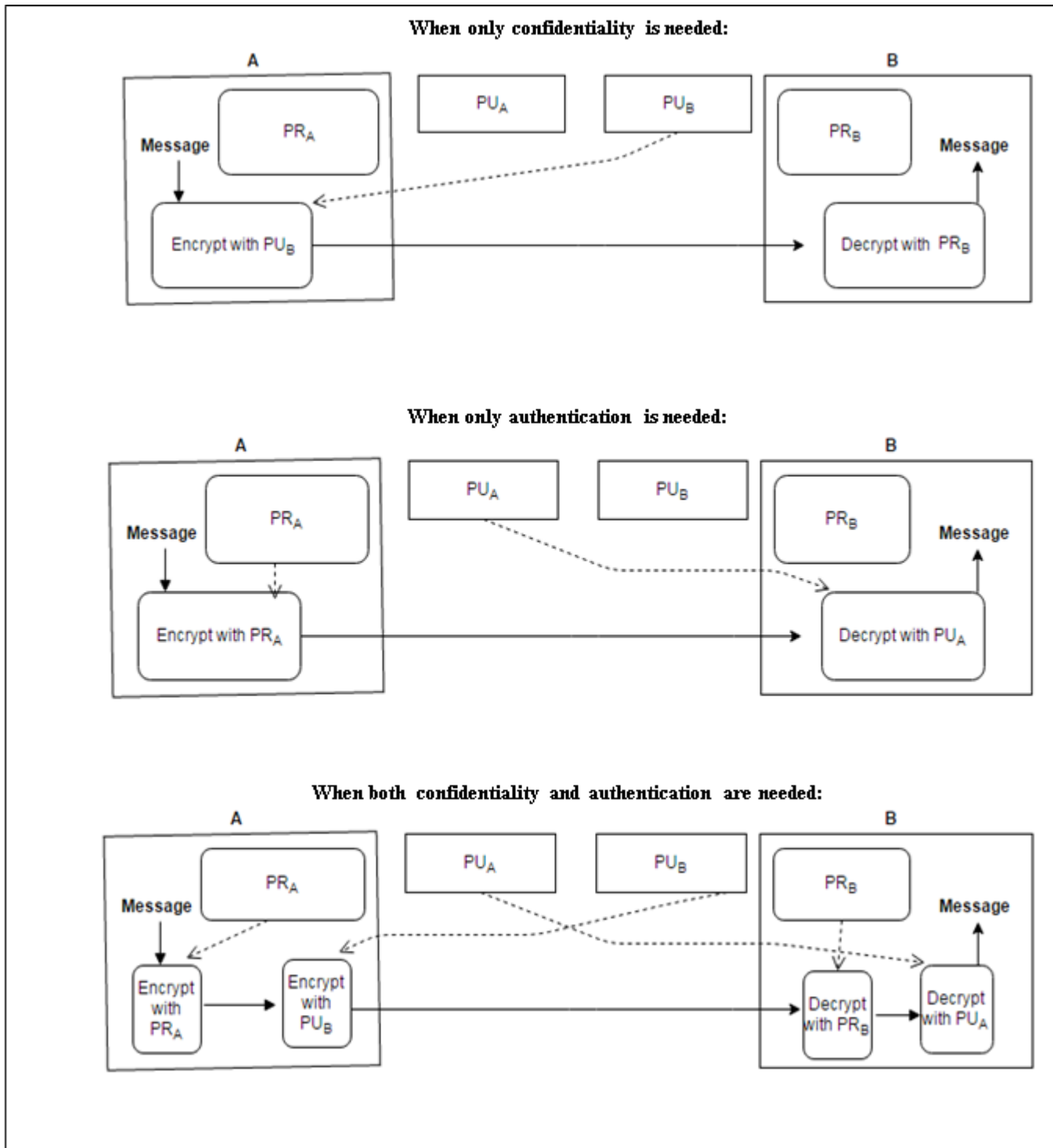


Figure 1: A wants to send a message/text to B

In figure 1 we have shown that how asymmetric key cryptography can be used for confidentiality and as well as for digital signatures. The steps undertaken by A to convert message into encrypted form C is given below: $C = E(PU_B, E(PR_A, Message))$ here E denoting encryption. B side to recover message from C are given $\rightarrow Message = D(PU_A, D(PR_B, C))$ here D denoting decryption. So, as we have seen that sender A encrypt message through its own private key PR_A which provides authentication. The sender A encrypting message with its personal private key PR_A gives authentication. This step comprises A putting digital signature on the message. Instead of applying the private key to the whole message, a dispatcher may also "sign" a message by applying private key to just a minute block of data that is resultant from the message to be sent. The cost compensated for achieving confidentiality and authentication simultaneously is that now the message must be processed 4 times in all for encryption and decryption. Two encryptions of message will do on the side of the sender and two decryptions on the side of the receiver. Every of these four steps involve independently the computationally complex public-key algorithm. Public-key cryptography does not make outdated the more conventional symmetric-key cryptography. Larger computational aloft is reason which connected with public-key cryptographic systems. However, public-key encryption has proved crucial for key management, for distributing the keys needed for the more conventional symmetric key encryption and decryption of the content, for digital signature applications, etc.

5 IMPLEMENTATION & KEY GENERATION

```

C:\Users\mypc\Desktop\Information Security\bin\Debug\Information Security
*****Information Security and Assurance*****
*****MS-SE F2016114012 Abdul Ghaffar*****
29 ENTER FIRST PRIME NUMBER
31 ENTER ANOTHER PRIME NUMBER
ENTER MESSAGE
SherazNaseer
***** POSSIBLE VALUES OF e AND d ARE *****
11 611
13 517
17 593
19 619
23 767
37 613
41 41
43 547
47 143
53 317
59 299
61 661
67 163
71 71
73 817
79 319
83 597
89 689
97 433
101 341
103 367
107 683
113 409
127 179
131 179
137 179
149 179
151 179
157 179
163 179
167 179
173 179
179 179
181 179
187 179
191 179
193 179
197 179
199 179
203 179
209 179
211 179
217 179
223 179
227 179
229 179
233 179
239 179
241 179
247 179
251 179
257 179
263 179
269 179
271 179
277 179
281 179
283 179
287 179
293 179
299 179
307 179
311 179
313 179
317 179
323 179
329 179
331 179
337 179
341 179
347 179
353 179
359 179
367 179
373 179
379 179
383 179
389 179
397 179
401 179
409 179
419 179
421 179
427 179
431 179
433 179
437 179
443 179
449 179
457 179
461 179
463 179
467 179
473 179
479 179
481 179
487 179
491 179
493 179
497 179
503 179
509 179
517 179
521 179
523 179
527 179
533 179
539 179
541 179
547 179
551 179
557 179
563 179
569 179
571 179
577 179
581 179
583 179
587 179
593 179
599 179
601 179
607 179
611 179
613 179
617 179
619 179
623 179
629 179
631 179
637 179
641 179
643 179
647 179
653 179
659 179
661 179
667 179
671 179
673 179
677 179
683 179
689 179
691 179
697 179
701 179
703 179
707 179
713 179
719 179
727 179
731 179
733 179
737 179
743 179
749 179
751 179
757 179
761 179
763 179
767 179
773 179
779 179
781 179
787 179
791 179
793 179
797 179
803 179
809 179
811 179
817 179
821 179
823 179
827 179
833 179
839 179
841 179
847 179
853 179
857 179
859 179
863 179
869 179
871 179
877 179
881 179
883 179
887 179
893 179
899 179
901 179
907 179
911 179
913 179
917 179
919 179
923 179
929 179
931 179
937 179
941 179
943 179
947 179
953 179
959 179
961 179
967 179
971 179
973 179
977 179
983 179
989 179
991 179
997 179
1003 179
1009 179
1013 179
1017 179
1021 179
1023 179
1027 179
1033 179
1039 179
1041 179
1047 179
1053 179
1057 179
1063 179
1069 179
1071 179
1073 179
1077 179
1081 179
1083 179
1087 179
1093 179
1097 179
1103 179
1109 179
1111 179
1117 179
1123 179
1129 179
1133 179
1137 179
1143 179
1149 179
1151 179
1157 179
1163 179
1169 179
1171 179
1173 179
1177 179
1183 179
1189 179
1193 179
1197 179
1201 179
1203 179
1207 179
1213 179
1217 179
1219 179
1223 179
1229 179
1231 179
1237 179
1241 179
1243 179
1247 179
1253 179
1259 179
1261 179
1267 179
1271 179
1273 179
1277 179
1283 179
1289 179
1291 179
1293 179
1297 179
1303 179
1307 179
1313 179
1317 179
1319 179
1323 179
1327 179
1329 179
1333 179
1337 179
1343 179
1349 179
1351 179
1357 179
1363 179
1369 179
1371 179
1373 179
1377 179
1383 179
1389 179
1391 179
1393 179
1397 179
1403 179
1409 179
1411 179
1417 179
1423 179
1429 179
1433 179
1437 179
1443 179
1449 179
1451 179
1457 179
1463 179
1469 179
1471 179
1473 179
1477 179
1483 179
1489 179
1493 179
1497 179
1503 179
1507 179
1513 179
1517 179
1519 179
1523 179
1529 179
1531 179
1537 179
1541 179
1543 179
1547 179
1553 179
1559 179
1561 179
1567 179
1571 179
1573 179
1577 179
1583 179
1589 179
1591 179
1593 179
1597 179
1603 179
1607 179
1613 179
1617 179
1619 179
1623 179
1627 179
1629 179
1633 179
1637 179
1643 179
1649 179
1651 179
1657 179
1663 179
1669 179
1671 179
1673 179
1677 179
1683 179
1689 179
1691 179
1693 179
1697 179
1703 179
1709 179
1711 179
1717 179
1723 179
1729 179
1733 179
1737 179
1743 179
1749 179
1751 179
1757 179
1763 179
1769 179
1771 179
1773 179
1777 179
1783 179
1789 179
1793 179
1797 179
1803 179
1807 179
1813 179
1817 179
1819 179
1823 179
1827 179
1829 179
1833 179
1837 179
1843 179
1849 179
1851 179
1857 179
1863 179
1869 179
1871 179
1873 179
1877 179
1883 179
1889 179
1891 179
1893 179
1897 179
1903 179
1907 179
1913 179
1917 179
1919 179
1923 179
1927 179
1929 179
1933 179
1937 179
1943 179
1949 179
1951 179
1957 179
1963 179
1969 179
1971 179
1973 179
1977 179
1983 179
1989 179
1993 179
1997 179
2003 179
2009 179
2011 179
2017 179
2023 179
2029 179
2033 179
2037 179
2043 179
2049 179
2051 179
2057 179
2063 179
2069 179
2071 179
2073 179
2077 179
2083 179
2089 179
2093 179
2097 179
2103 179
2107 179
2113 179
2117 179
2119 179
2123 179
2127 179
2129 179
2133 179
2137 179
2143 179
2149 179
2151 179
2157 179
2163 179
2169 179
2171 179
2173 179
2177 179
2183 179
2189 179
2193 179
2197 179
2203 179
2207 179
2213 179
2217 179
2219 179
2223 179
2227 179
2229 179
2233 179
2237 179
2243 179
2249 179
2251 179
2257 179
2263 179
2269 179
2271 179
2273 179
2277 179
2283 179
2289 179
2293 179
2297 179
2303 179
2307 179
2313 179
2317 179
2319 179
2323 179
2327 179
2329 179
2333 179
2337 179
2343 179
2349 179
2351 179
2357 179
2363 179
2369 179
2371 179
2373 179
2377 179
2383 179
2389 179
2393 179
2397 179
2403 179
2407 179
2413 179
2417 179
2419 179
2423 179
2427 179
2429 179
2433 179
2437 179
2443 179
2449 179
2451 179
2457 179
2463 179
2469 179
2471 179
2473 179
2477 179
2483 179
2489 179
2493 179
2497 179
2503 179
2507 179
2513 179
2517 179
2519 179
2523 179
2527 179
2529 179
2533 179
2537 179
2543 179
2549 179
2551 179
2557 179
2563 179
2569 179
2571 179
2573 179
2577 179
2583 179
2589 179
2593 179
2597 179
2603 179
2607 179
2613 179
2617 179
2619 179
2623 179
2627 179
2629 179
2633 179
2637 179
2643 179
2649 179
2651 179
2657 179
2663 179
2669 179
2671 179
2673 179
2677 179
2683 179
2689 179
2693 179
2697 179
2703 179
2707 179
2713 179
2717 179
2719 179
2723 179
2727 179
2729 179
2733 179
2737 179
2743 179
2749 179
2751 179
2757 179
2763 179
2769 179
2771 179
2773 179
2777 179
2783 179
2789 179
2793 179
2797 179
2803 179
2807 179
2813 179
2817 179
2819 179
2823 179
2827 179
2829 179
2833 179
2837 179
2843 179
2849 179
2851 179
2857 179
2863 179
2869 179
2871 179
2873 179
2877 179
2883 179
2889 179
2893 179
2897 179
2903 179
2907 179
2913 179
2917 179
2919 179
2923 179
2927 179
2929 179
2933 179
2937 179
2943 179
2949 179
2951 179
2957 179
2963 179
2969 179
2971 179
2973 179
2977 179
2983 179
2989 179
2993 179
2997 179
3003 179
3007 179
3013 179
3017 179
3019 179
3023 179
3027 179
3029 179
3033 179
3037 179
3043 179
3049 179
3051 179
3057 179
3063 179
3069 179
3071 179
3073 179
3077 179
3083 179
3089 179
3093 179
3097 179
3103 179
3107 179
3113 179
3117 179
3119 179
3123 179
3127 179
3129 179
3133 179
3137 179
3143 179
3149 179
3151 179
3157 179
3163 179
3169 179
3171 179
3173 179
3177 179
3183 179
3189 179
3193 179
3197 179
3203 179
3207 179
3213 179
3217 179
3219 179
3223 179
3227 179
3229 179
3233 179
3237 179
3243 179
3249 179
3251 179
3257 179
3263 179
3269 179
3271 179
3273 179
3277 179
3283 179
3289 179
3293 179
3297 179
3303 179
3307 179
3313 179
3317 179
3319 179
3323 179
3327 179
3329 179
3333 179
3337 179
3343 179
3349 179
3351 179
3357 179
3363 179
3369 179
3371 179
3373 179
3377 179
3383 179
3389 179
3393 179
3397 179
3403 179
3407 179
3413 179
3417 179
3419 179
3423 179
3427 179
3429 179
3433 179
3437 179
3443 179
3449 179
3451 179
3457 179
3463 179
3469 179
3471 179
3473 179
3477 179
3483 179
3489 179
3493 179
3497 179
3503 179
3507 179
3513 179
3517 179
3519 179
3523 179
3527 179
3529 179
3533 179
3537 179
3543 179
3549 179
3551 179
3557 179
3563 179
3569 179
3571 179
3573 179
3577 179
3583 179
3589 179
3593 179
3597 179
3603 179
3607 179
3613 179
3617 179
3619 179
3623 179
3627 179
3629 179
3633 179
3637 179
3643 179
3649 179
3651 179
3657 179
3663 179
3669 179
3671 179
3673 179
3677 179
3683 179
3689 179
3693 179
3697 179
3703 179
3707 179
3713 179
3717 179
3719 179
3723 179
3727 179
3729 179
3733 179
3737 179
3743 179
3749 179
3751 179
3757 179
3763 179
3769 179
3771 179
3773 179
3777 179
3783 179
3789 179
3793 179
3797 179
3803 179
3807 179
3813 179
3817 179
3819 179
3823 179
3827 179
3829 179
3833 179
3837 179
3843 179
3849 179
3851 179
3857 179
3863 179
3869 179
3871 179
3873 179
3877 179
3883 179
3889 179
3893 179
3897 179
3903 179
3907 179
3913 179
3917 179
3919 179
3923 179
3927 179
3929 179
3933 179
3937 179
3943 179
3949 179
3951 179
3957 179
3963 179
3969 179
3971 179
3973 179
3977 179
3983 179
3989 179
3993 179
3997 179
4003 179
4007 179
4013 179
4017 179
4019 179
4023 179
4027 179
4029 179
4033 179
4037 179
4043 179
4049 179
4051 179
4057 179
4063 179
4069 179
4071 179
4073 179
4077 179
4083 179
4089 179
4093 179
4097 179
4103 179
4107 179
4113 179
4117 179
4119 179
4123 179
4127 179
4129 179
4133 179
4137 179
4143 179
4149 179
4151 179
4157 179
4163 179
4169 179
4171 179
4173 179
4177 179
4183 179
4189 179
4193 179
4197 179
4203 179
4207 179
4213 179
4217 179
4219 179
4223 179
4227 179
4229 179
4233 179
4237 179
4243 179
4249 179
4251 179
4257 179
4263 179
4269 179
4271 179
4273 179
4277 179
4283 179
4289 179
4293 179
4297 179
4303 179
4307 179
4313 179
4317 179
4319 179
4323 179
4327 179
4329 179
4333 179
4337 179
4343 179
4349 179
4351 179
4357 179
4363 179
4369 179
4371 179
4373 179
4377 179
4383 179
4389 179
4393 179
4397 179
4403 179
4407 179
4413 179
4417 179
4419 179
4423 179
4427 179
4429 179
4433 179
4437 179
4443 179
4449 179
4451 179
4457 179
4463 179
4469 179
4471 179
4473 179
4477 179
4483 179
4489 179
4493 179
4497 179
4503 179
4507 179
4513 179
4517 179
4519 179
4523 179
4527 179
4529 179
4533 179
4537 179
4543 179
4549 179
4551 179
4557 179
4563 179
4569 179
4571 179
4573 179
4577 179
4583 179
4589 179
4593 179
4597 179
4603 179
4607 179
4613 179
4617 179
4619 179
4623 179
4627 179
4629 179
4633 179
4637 179
4643 179
4649 179
4651 179
4657 179
4663 179
4669 179
4671 179
4673 179
4677 179
4683 179
4689 179
4693 179
4697 179
4703 179
4707 179
4713 179
4717 179
4719 179
4723 179
4727 179
4729 179
4733 179
4737 179
4743 179
4749 179
4751 179
4757 179
4763 179
4769 179
4771 179
4773 179
4777 179
4783 179
4789 179
4793 179
4797 179
4803 179
4807 179
4813 179
4817 179
4819 179
4823 179
4827 179
4829 179
4833 179
4837 179
4843 179
4849 179
4851 179
4857 179
4863 179
4869 179
4871 179
4873 179
4877 179
4883 179
4889 179
4893 179
4897 179
4903 179
4907 179
4913 179
4917 179
4919 179
4923 179
4927 179
4929 179
4933 179
4937 179
4943 179
4949 179
4951 179
4957 179
4963 179
4969 179
4971 179
4973 179
4977 179
4983 179
4989 179
4993 179
4997 179
5003 179
5007 179
5013 179
5017 179
5019 179
5023 179
5027 179
5029 179
5033 179
5037 179
5043 179
5049 179
5051 179
5057 179
5063 179
5069 179
5071 179
5073 179
5077 179
5083 179
5089 179
5093 179
5097 179
5103 179
5107 179
5113 179
5117 179
5119 179
5123 179
5127 179
5129 179
5133 179
5137 179
5143 179
5149 179
5151 179
5157 179
5163 179
5169 179
5171 179
5173 179
5177 179
5183 179
5189 179
5193 179
5197 179
5203 179
5207 179
5213 179
5217 179
5219 179
5223 179
5227 179
5229 179
5233 179
5237 179
5243 179
5249 179
5251 179
5257 179
5263 179
5269 179
5271 179
5273 179
5277 179
5283 179
5289 179
5293 179
5297 179
5303 179
5307 179
5313 179
5317 179
5319 179
5323 179
5327 179
5329 179
5333 179
5337 179
5343 179
5349 179
5351 179
5357 179
5363 179
5369 179
5371 179
5373 179
5377 179
5383 179
5389 179
5393 179
5397 179
5403 179
5407 179
5413 179
5417 179
5419 179
5423 179
5427 179
5429 179
5433 179
5437 179
5443 179
5449 179
5451 179
5457 179
5463 179
5469 179
5471 179
5473 179
5477 179
5483 179
5489 179
5493 179
5497 179
5503 179
5507 179
5513 179
5517 179
5519 179
5523 179
5527 179
5529 179
5533 179
5537 179
5543 179
5549 179
5551 179
5557 179
5563 179
5569 179
5571 179
5573 179
5577 179
5583 179
5589 179
5593 179
5597 179
5603 179
5607 179
5613 179
5617 179
5619 179
5623 179
5627 179
5629 179
5633 179
5637 179
5643 179
5649 179
5651 179
5657 179
5663 179
5669 179
5671 179
5673 179
5677 179
5683 179
5689 179
5693 179
5697 179
5703 179
5707 179
5713 179
5717 179
5719 179
5723 179
5727 179
5729 179
5733 179
5737 179
5743 179
5749 179
5751 179
5757 179
5763 179
5769 179
5771 179
5773 179
5777 179
5783 179
5789 179
5793 179
5797 179
5803 179
5807 179
5813 179
5817 179
5819 179
5823 179
5827 179
5829 179
5833 179
5837 179
5843 179
5849 179
5851 179
5857 
```


References:

- [1] Symmetric and asymmetric encryption
- [2] GJ Simmons - ACM Computing Surveys (CSUR), 1979 - dl.acm.org
- [3] Secure Communication using Symmetric and Asymmetric Cryptographic Techniques
- [4] OM Barukab, AI Khan, MS Shaik... - International ..., 2012 - search.proquest.com
- [5] A comprehensive literature review of asymmetric key cryptography algorithms for establishment of the existing gap JN Gaithuru, M Bakhtiari, M Salleh... - ... (MySEC), 2015 9th ..., 2015 - ieeexplore.ieee.org
- [6] A survey of lightweight-cryptography implementations
- [7] A comparative survey of symmetric and asymmetric key cryptography S Chandra, S Paira, SS Alam... - Electronics, ..., 2014 - ieeexplore.ieee.org
- [8] Double Chaining Algorithm A Secure Symmetric-key Encryption Algorithm
- [9] A comparative survey of symmetric and asymmetric key cryptography