Scientific and Practical Cyber Security Journal (SPCSJ) 10(1): 121 – 140 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

AN ANALYSIS OF THE ASYMMETRIC RANDOM NOISY RSA ENCRYPTION SCHEME

Edgar Rangel Lugo[1], Cinthya Maybeth Rangel Ríos[1], Kevin Uriel Rangel Ríos[1], Leticia Roque Correa[1], Aracely Salgado Mendoza[1], César Del Ángel Rodríguez Torres[1], Leonel González Vidales[1] and Mauricio De La Cruz Ramos García[1]

[1]Tecnológico Nacional de México. Instituto Tecnológico de Ciudad Altamirano

ABSTRACT: Digital data theft represents a major threat to organizations. This research examines cybersecurity approaches that integrate random noise mechanisms bases on Artificial Intelligence (IA). We introduce an innovative solution called the random noisy RSA strategy, which injects noise into ciphertext to enhance security. Our method caters to the demand for adaptive encryption techniques, producing distinct ciphertexts for identical plaintexts. We evaluate its performance against four RSA (Rivest-Shamir-Adleman) variations, demonstrating increased noise injection and promising results. Such methods could impede decryption attempts by cybercriminals, presenting a fresh way to strengthen data protection. Tests confirm that random noise-based strategies are effective at mitigating cyber risks. Our research equips organizations with a valuable resource to safeguard their digital data.

KEYWORDS*:* *Random noisy strategies, dynamic encryption methods, applications of AI, cybersecurity strategies.*

1. INTRODUCTION

A cybersecurity strategy is inadequate if vulnerable to cybercriminal attacks (Delman 2004; Kalsi et al. 2018; Mendoza 2008; Rangel and Rangel 2024a, 2025a; Rangel et al. 2025a, 2025b, 2025c), leading to digital data theft (Rangel et al. 2023; Rangel et al. 2025c) and financial losses (Rangel and Rangel 2024a, 2024b; Rangel et al. 2024, 2025a, 2025c). Approaches include regular strategy replacement (Rangel and Rangel 2024a), dynamic encryption (Rangel et al. 2025a), and noisy injection (Rangel and Rangel 2025a; Rangel et al. 2023, 2024, 2025a, 2025b). This study focuses on encryption methods with noisy injection (Rangel et al. 2025c), which transform plaintext into ciphertext (Rangel et al. 2025c) and are dynamic if they produce distinct results (Rangel et al. 2025c). Encryption algorithms can be categorized as either symmetric, using a single secret key, or asymmetric, utilizing a pair of keys (private and public). Symmetric encryption algorithms include DES: Data Encryption Standard (Baklaga 2024; Barranco and Galindo 2022; Bavdekar et al. 2023; Dhany et al. 2018; Gómez et al. 2012; Kumar and Sharma 2021; Mendoza 2008; Progress; Software Corporation Telerik 2022; Rodríguez 2020), 3DES or TripleDES: Triple Data Encryption Standard (Baklaga 2024; Bavdekar et al. 2023; Gómez et al. 2012; Mendoza 2008; Van and Jajodia 2011; Van-Tilborg 2005), GOST: GOsudarstvennyi STandard (Alvarez 2019; Courtois 2012; Dhany et al. 2018; Dunkelman et al. 2023; Fulgueira et al. 2015; Gómez et al. 2012; Gundaram 2024; Ishchukova et al. 2020; Nagaraj and Srinadth 2015; Oppliger 2005; Rangel and Rangel 2025a; Rangel et al. 2024, 2025b; Stinson and Paterson 2019; Van-Tilborg 2005), IDEA: International Data Encryption Algorithm (Gundaram 2024; Van-Tilborg 2005), AES: Advanced Encryption Standard (Baklaga 2024; Barranco and Galindo 2022; Bavdekar et al. 2023; Daemen and Rijmen 2002; Ishchukova et al. 2020; Muhammed et al. 2024; NIST 2001; Progress Software Corporation Telerik 2022; Rahman and Hossain 2021; Rodríguez 2020; Saini et al. 2023; Singh and Kumar 2022; Van-Tilborg 2005), Blowfish (Baklaga 2024; Bavdekar et al. 2023; Schneier 1994; Schneier 2000; AL-Maqtari and AL-Maqtari 2024; Muhammed et al. 2024), Twofish (AL-Maqtari and AL-Maqtari 2024; Muhammed et al. 2024), CAST: Carlisle Adams and Stafford Tavares (Rangel et al. 2025d; Wang et al. 2017), Camellia (Aoki et al. 2000; Oppliger 2005; Rangel and Rangel 2025a; Sami-Sulaiman and Hammood 2025), Salsa20 (Garai and Dey 2024; Rangel et al. 2025e), ChaCha20 (Garai and Dey 2024; Rangel et al. 2025f) and RC: Rivest Cipher (Mendoza 2008; Mohammed et al. 2025; Rambe 2024; Van-Tilborg 2005). Studies (Rangel et al. 2025a, 2025c) show these algorithms produce static results but aren't

inherently insecure (Rangel et al. 2025a). This research does not address symmetric algorithms, as they can be explored in the future. Asymmetric encryption algorithms include RSA (Baklaga 2024; Barranco and Galindo 2022; Bavdekar et al. 2023; Dang and Le 2022; Gómez et al. 2012; Luciano and Prichett 1987; Oppliger 2005; Rahman and Hossain 2021; Rangel et al. 2025a, 2025b, 2025c; Rodríguez 2020; Stinson and Paterson 2019; Van-Tilborg 2005), ECC (Baker and Schiller 2015; Baklaga 2024; Bavdekar et al. 2023; Hankerson et al. 2004; Montgomery 1987; NIST 2013; Oppliger 2005; Rangel et al. 2025a, 2025b, 2025c; Stinson and Paterson 2019; Van-Tilborg 2005) and ElGamal (Barranco and Galindo 2022; Oppliger 2005; Stinson and Paterson 2019; Van-Tilborg 2005). These schemes require both private and public keys to operate. This research aims to employ noisy injection based on RSA-1024, RSA-2048, RSA-4096 and RSA-8192 variants (Baklaga 2024; Barranco and Galindo 2022; Bavdekar et al. 2023; Dang and Le 2022; Gómez et al. 2012; Luciano and Prichett 1987; Mendoza 2008; Oppliger 2005; Rahman and Hossain 2021; Rangel et al. 2025a, 2025b, 2025c; Saini et al. 2023; Stinson and Paterson 2019; Van-Tilborg 2005). Recent research (Rangel et al. 2025a, 2025b; Rangel and Rangel 2024b) have reported dynamic encryption results when these asymmetric alternatives were employed. However, algorithms like AES and RSA are vulnerable to quantum attacks (Baklaga 2024; Bavdekar et al. 2023; Iavich et al. 2024; Fuegner 2024; Sengupta and Ghosh 2023; Thakur and Kumar 2011). Quantum computing reduces cryptosystem security (Baklaga 2024). Dynamic encryption is an alternative to enhance security (Rangel et al. 2023; Rangel and Rangel 2024a). This study proposes additional security measures for RSA with noise injection (Rangel et al. 2025a). Dynamic encryption methods with noisy injection (Rangel and Rangel 2024a, 2024b, 2025a; Rangel et al. 2023, 2024, 2025a, 2025b, 2025c) are promising for enhancing security. Noise injection adds extra characters to ciphertext (Rangel et al. 2025c, 2025f). Artificial Intelligence (AI) is used in cryptography (Rangel 2002, 2022; Rangel and Rangel 2024b; Rangel et al. 2024, 2025a, 2025c) with methods like genetic algorithms or GA (Clark 1994; Delman 2004; Griindlingh and Van-Vuuren 2003; Kalsi et al. 2018; Kuncheva and Jain 1999; Matthews 1993; Rangel et al. 2023, 2024; Reddaiah 2019; Sebas 2023; Skalak 1994) and artificial neural networks (Bruzzone and Serpico 1997; Goodfellow et al. 2021; Murphy 2022). AI is used in cryptography (Iyengar et al. 2021; Singh et al. 2021) with studies on asymmetric and symmetric encryption (Mendoza 2008), pairing functions (Reddaiah 2016), and other research based on GA (Delman 2004; Matthews 1993; Clark 1994; Griindlingh and Van-Vuuren 2003; Rodríguez 2020). There are also studies on AI-cryptanalysis (Dang and Le 2022; Liu and Wang 2022). According to (Rangel and Rangel 2024a, 2024b, 2025a; Rangel et al. 2023, 2024, 2025a, 2025b, 2025c), the random noisy strategies include approaches like pseudo-hexadecimal GA (Rangel et al. 2023, 2024, 2025c) and combining noisy injection with 1-NN (Barandela et al. 2003; Cover and Hart 1967; Lewis and Catlett 1994; Rangel 2002, 2022; Rangel and Rangel 2024b). These strategies enhance digital data security but require more storage space and have only been employed with plaintext. In a similar context, the random Caesar II (Rangel and Rangel 2024a, 2024b, 2025a; Rangel et al. 2025a, 2025b) is a random noisy strategy that uses less disk space than the pseudo-hexadecimal schema. The random Caesar methodology injects noise into plaintext and ciphertext using a two-stage approach. It is based on the traditional Caesar algorithm (Barranco and Galindo 2022; Gómez et al. 2012; Rangel and Rangel 2024a; Rangel et al. 2023), but with dynamic encryption capabilities using AI (Rangel et al. 2025a). Hence, random Caesar II can be computed as follows: $C_i = S_i + K_i \bmod N$. Where S_i and K_i are the plaintext and shifting, respectively. AI is used in random Caesar encryption methods (Rangel and Rangel 2024a, 2024b; Rangel et al. 2023, 2025b) with modes like mod 9 & mod 255 (Rangel et al. 2025b), mod 95 (Rangel and Rangel 2024a, 2024b; Rangel et al. 2023), and mod 120 (Rangel and Rangel 2024a, 2025a; Rangel et al. 2025a, 2025b, 2025d, 2025e, 2025f). In its first phase, these schemes use a random and heuristic approach or GA to determine the K_i vector and encryption alphabet size, as explained by other authors (Rangel et al. 2024; 2025b; Rangel and Rangel 2025a, 2025e, 2025f, 2025g) in previous works, which justifies the use of AI. The second phase of the random Caesar scheme confuses cybercriminals (Rangel and Rangel 2024a) and involves calculating the final package (Rangel et al. 2025a) by injecting noise characters as follows: $\text{FinalPackage} = C_i + \text{OrdChr}(K_i) + \text{OrdChr}(C_i)$. Where C_i and OrdChr are the ciphertext and shifting byte or noisy character, respectively, as explained in other research (Rangel et al. 2025d, 2025e, 2025f, 2025g). The random Caesar II mod 120 is used as a random noisy strategy (Rangel and Rangel 2025a; Rangel et al. 2025a, 2025b) in combinations with

standard encryption, generating alternatives like random noisy DES, random noisy 3DES, random noisy AES-256, random noisy RC4, random noisy Blowfish, random noisy WEP, random noisy RSA-2048, and random noisy ECIES SECP-256-R1 (Rangel et al. 2025a). Similarly, the random noisy CAST-128 (Rangel et al. 2025d), random noisy GOST R 34.12-2015 (Rangel et al. 2025b), random noisy Camellia (Rangel and Rangel 2025a), random noisy ChaCha20 (Rangel et al. 2025f), and random noisy Salsa20 (Rangel et al. 2025e). Other strategies such as reduced random Caesar and reduced random mutation (Rangel and Rangel 2024a; Rangel et al. 2025g) aim to camouflage and reduce ciphertext size. This work examined random variants of RSA with random noise (random noisy RSA variants). Applying noisy injection with random noisy strategies (Rangel and Rangel 2024a, 2025a; Rangel et al. 2025a, 2025b) is recommended due to its correlation with dynamic encryption performance. This research builds on previous work on random noisy alternatives (Rangel and Rangel 2025a; Rangel et al. 2025a, 2025b) and aims to apply random noise strategies to RSA variants to enhance cybersecurity (Rangel et al. 2025c). This paper compares the standard RSA encryption algorithm with random variants of noisy RSA schemes. The goal is to evaluate dynamic encryption as a means to increase the security performance of digital data (Rangel and Rangel 2025a; Rangel et al. 2025a, 2025b). This study contributes to AI-based cryptography by examining random noisy strategies (Rangel and Rangel 2024a, 2024b; Rangel et al. 2023, 2024, 2025a). The random Caesar II approach (Rangel and Rangel, 2024a) generates random values but poses no issues in practical domains (Rangel et al. 2025a). Performance is measured by average accuracy or global accuracy (Barandela et al. 2003; Lewis and Catlett 1994; Rangel 2002, 2022). This paper presents experimental results on using random noisy strategies for dynamic encryption (Rangel and Rangel 2024a; Rangel et al. 2025a). The study proposes random variants of RSA with random noise (random noisy RSA variants) as a dynamic alternative for data encryption. It is hypothesized that they can be difficult for cybercriminals to decrypt.

2. RELATED THEORETICAL AND EXPERIMENTAL METHODS

Static encryption does not provide sufficient data security guarantees. A *dynamic encryption* solution is advisable (Rangel and Rangel 2024a). We evaluated *dynamic encryption* approaches with *random noisy* (Rangel et al. 2025a) to address digital data theft. This research is experimental and exploratory, introducing *random noisy RSA variants* (*RSA-1024, RSA-2048, RSA-4096* and *RSA-8192*). Experiments were conducted on a personal computer and a mobile device, with consistent results on Windows and Android, respectively. The datasets used were *training samples* or *TS* (Barandela et al. 2003; Rangel 2002, 2022; Rangel and Rangel 2025a; Rangel et al. 2025b) with 1000 instances. Each *pattern* includes *ciphertext*, *encryption time*, *decryption time*, *error* rate, and class *label*. The format is *TP = [(Test1, Test2), TC, TD, Error, Label]*. Each encryption strategy was executed using the updated *TS* format. *Table 1* provides the *mean* and *standard deviation* for a specific case (Rangel and Rangel 2025a; Rangel et al. 2025a, 2025b).

First, the *standard asymmetric encryption* algorithms, specifically *RSA* and variants, were tested and implemented using the *Python* language. Several *Python libraries* were imported as follows: `from Crypto.PublicKey import RSA ; from Crypto.Cipher import PKCS1_OAEP ; from cryptography.hazmat.primitives.asymmetric import ec ; from cryptography.hazmat.primitives import serialization ; Si = ''.join([ chr(9619), 'W', 'e', 'l', 'c', 'o', 'm', 'e', chr(9619), chr(65533)])`. Given `Si = '▓Welcome▓?'`, we can proceed with the analysis. To obtain the *ciphertext* based on the *RSA* algorithm, the following instruction can be applied: `Ci = A (plaintext).hex() ; print(Ci)`. Under these conditions, valid *parameters* for generating *ciphertext* with the *RSA* algorithm can be determined as follows: `FilePublicKey = 'publicrsa.txt' ; FilePrivateKey = 'privatersa.txt' ; Key = '00000000000000000000000000000001' ; priKey = RSA.importKey(open(FilePrivateKey , 'rb').read() , passphrase=Key.encode()) ; PK = RSA.importKey (open(FilePublicKey, 'rb').read() , passphrase=Key.encode()) ; Qi = PKCS1_OAEP.new(PK) ; plaintext = Si.encode() ; A = Qi.encrypt(plaintext) ; Ci = (A.hex()) ; print(Ci)`. It is necessary to include instructions in the source code to use `Ci` with asymmetric algorithm *RSA*. Public and private keys are required, generated before using `Ci`. The

private key can be created in *PEM (Privacy-Enhanced Mail)* format with *PKCS1_OAEP (Public Key Cryptography Standard with Optimal Asymmetric Encryption Padding)*. For example: `open( FilePrivateKey ,'wb').write( priKey.export_key( format=F , passphrase=Key.encode()))`. To generate the *public key*, the following instruction can be used: `open( FilePublicKey ,'wb').write( PK.publickey().export_key( format=F , passphrase= Key.encode() ) )`. The above procedure involves setting or declaring a series of values, as follows: `FilePublicKey = 'publicrsa.txt' ; FilePrivateKey = 'privatersa.txt'; Key = '00000000000000000000000000000001' ; F = 'PEM' ; N = 2048 ; priKey = RSA.generate(N) ; PK = priKey.publickey()`. Therefore, for *RSA* data decryption, it can be obtained as follows: `print ( ( ( PKCS1_OAEP.new(priKey)).decrypt(bytes.fromhex(Ci)) ).decode() )`. The object `A` refers to the encryption algorithm (*RSA*). The *secret key* is used to generate the *private key*. For *RSA*, the *private key* is generated with `RSA.generate(N)` and the *public key* with `priKey.publickey()`. The *keys* are saved to files and read with `RSA.importKey()`.

The second encryption strategy involves random noisy alternatives for dynamic data encryption (Rangel and Rangel 2024a; Rangel et al. 2025a). We propose random noisy RSA variants, being implemented in Python and tested with noise injection. The results were evaluated using modified cross-validation (Rangel and Rangel 2024a). According to (Rangel et al. 2025a) presents the framework for applying noise injection to the ciphertext and explains the procedure for calculating random noisy strategies. The calculation is performed as follows: $RandomNoisy_i$ = Char (Ord (StandardEncryptioni) + Ord(K_i)) & Char (K_i) & Char ($StandardEncryption_i$) mod 120. Accordind to (Rangel and Rangel 2024a), this process simplifies the substitution of plaintext with ciphertext. In this study, we use the same strategy to generate the ciphertext of $StandardEncryption_i$. The random noisy RSA strategy is implemented and calculated using the instruction: $RandomNoisyRSA\mathbf{xNx}_i$ = Char (Ord (StandardRSA**xNx**$Encryption_i$) + Ord(K_i)) & Char (K_i) & Char (StandardRSA**xNx**$Encryption_i$) mod 120. Here, the + operator represents the sum function and the & operator represents concatenation. The shift vector K_i contains random integers between 30 and 150 (using mod 120). The StandardRSA**xNx**$Encryption_i$ represents a ciphertext obtained using standard asymmetric encryption algorithm (RSA), as described in (Rangel et al. 2025a). The values **xNx** and **xBitsx** have the same range of values as N and Bits, respectively. The values stored in $RandomNoisyRSA\mathbf{xNx}_i$ corresponds to the noisy ciphertext calculated by the RSA algorithm. The Ord function returns the ordinal value of a character or integer, and the Char function converts a value to its corresponding character representation in ASCII or UTF-8. In the random noisy proposals, a standard algorithm encrypts the plaintext and applies random Caesar II mod 120 to the ciphertext, adding security (Rangel and Rangel 2025a; Rangel et al. 2025a, 2025b). It is advisable to apply noisy injection to only a portion of the ciphertext to avoid drawing attention (Rangel et al. 2025a). These strategies use random Caesar II mod 120 on standard ciphertext (Rangel and Rangel 2024a; Rangel et al. 2025a). The random noisy strategies are dynamic encryption alternatives (Rangel and Rangel 2024a), effective in producing dynamic ciphertext and improving security. The random Caesar II mod 120 approach uses AI to determine the shift vector K_i (Rangel et al. 2025a), ensuring dynamic results with each execution. Although the standard asymmetric RSA encryption algorithm generates dynamic ciphertext outputs, applying a random noisy strategy to the RSA ciphertext results in a double dynamic random ciphertext scheme. This provides an additional layer of safety for digital data. The heuristic method is similar to the genetic algorithm (GA) selection process, considered an AI application (Rangel et al. 2025a, 2025c). The GA selection procedure is used for alphabet selection with mod 120 and shift vector K_i (Rangel and Rangel 2024a; Rangel et al. 2025a). The K_i range is limited to avoid exceeding the ASCII table maximum. We excluded reduced random Caesar and reduced random mutation from this study. We used a modified cross-validation approach (Rangel and Rangel 2024a, 2025a; Rangel et al. 2025a, 2025b) to evaluate the results. Noise injection based on random noisy strategy can be a valuable security measure.

3. RESULTS AND DISCUSSION

Each TS was used separately for experiments. Modified five-fold cross-validation (Rangel and Rangel 2024a) was applied to each TS, allowing comparison with other research (Rangel et al. 2025a, 2025b; Rangel and Rangel, 2025a). The method divides the TS into five subsamples (20% each) for model evaluation (Rangel and Rangel 2025a). This process is repeated five times to determine the standard deviation after calculating the average or global accuracy (Lewis and Catlett 1994). This scheme simulates the estimated error in various environments, excluding part of the TS, resulting in a more convergent outcome with optimistic bias (Rangel and Rangel 2025a). The method evaluates the estimated error and other numerical characteristics of the TS. The error percentage is calculated when the decrypted ciphertext does not match the plaintext. The process is repeated five times, allowing calculation of the mean and standard deviation of TC, TD, and overall error percentage. The experimentation compared standard asymmetric RSA encryption algorithm and the random noisy RSA variants (Rangel et al. 2025a), being applied to the ciphertext. The four random noisy RSA variants were tested to inject noise into the ciphertext. The overall average results were calculated with the updated cross-validation method (Rangel and Rangel 2024a, 2025a, 2025b; Rangel and Rangel 2025a, 2025b). The results (TC, TD, and error) are in Table 1, with standard deviation in parentheses. The RSA algorithm used PEM format with size variants (1024, 2048, 4096, 8192) and secret key '00000000000000000000000000000001'. PKCS1_OAEP padding (padding=16) were used, generating hexadecimal ciphertext.

The *RSA-1024* experiments utilized a *public key* with a value of '-----BEGIN PUBLIC KEY-----
Proc-Type: 4,ENCRYPTED DEK-Info: DES-EDE3-CBC,85B707D3B7B61C77
A4uM2nAbBKPIkT2XaSfQKyxhooa29ZMyt0tPIKqrIbrmpgf9Jdbrv8EeZXqfD14TsyVW9QmsFHyFLQ50SO2
eRtPeXp4C6iojUoVGR/jOZiogMTsbV3Q91pNXuEcvQqMObU8T25totUCT36W57kH/9oXKPh4yrV4eHrfhP1
WhnIl6TXy5f8NoT7il+xLwoGdBqtvzWAP47VnG8ET1iKYPM4YGWrmwYhBl -----END PUBLIC KEY-----
'. For the *RSA-1024* standard, the *private key* used was: '-----BEGIN RSA PRIVATE KEY----- Proc-
Type:4,ENCRYPTED DEK-Info:DES-EDE3-CBC, 56E5EFC93EF95E17uVfKw1zBX5tCXx9mtdL
1Yp1r2JAoCfc778czYMuwORH240z6kIg5l+1PuwfA55RXHE5W3icsqY+0tcBDcyt70w40eA1fTLjgac/mq
fgGMi8KOH1a0AYqsvTNpo54yA4wKeC8we/CJTNWLVYSbSk8FJweXLd0sOvdtBcZfrk2kNjm1LQWhsMJEfnj69Y3BH7SuM1
ZKrzg2MtXqdrTMUEc/0Uy8VSkNaQzYNKxvdtQSanMJLSLV2kF+91cNrM2oGRGGNGAmns3UBz+mgrdibP0HJW/z1p5YEgmK
Kw/05aKe1UpaWUST+t2h8v7d9FrTqGKKwJmq1M3YdEpb+ttQaPWI2RlJgk+WuxansLTqkvTubMzmgkkTpIvztQx19SVZjL
C+0KI9csBQ8iSFIjT3t70oPnTWRKgHhh4jqrUOQm5hvnIR5meDdHKmp5Hefwk+N+RqEVgIQ69N6NSLENTkEyCZtCWQyPCL
v5Nm4RLXytXDZYo7ue/34o00yeqz6rYR2g3TMoLY7i5LqOAY3RyjQh5G2tJSDNYwlOGcyuqIhd9AQto9DC5kHGR+gQOdsB
zZ+a2lNTpSDBOVQ2VnBF2EeQ4ys8qC43q5qrUGQoMLQ90fyWI0dyNZLP/2/eh9ZrImkQMwuLzt6ExLnseshi1D3k26H2hv
cKKpq2ncxLYObJlUU9OzrCBhWBTMWUJF0QkNboCyQu7a/kscJiisQj12EifIPNbJ4AjsB5NKFL3McjXhPCkchsmbqd0jp/
uo0sfofzeROT7DpHY+8u+EGr48+lhriFagUxulEJPoq5uc15+G+/5ctHqW+vkpg== -----END RSA PRIVATE KEY----
- '.

Tab.1*. Encryption/Decryption Performance and Error Analysis of RSA Variants.*

Encryption strategy	Test 1	Test 2	TC	TD	Error
RSA-1024	08be174ab81dd8fa2b4e9eb291bd72d07a3b368a12ed4b0c89d3471f89cd4cbc2386041a3704d313ac17f21e8379dc9b4feb4b75aadece0f3ba9899b8f3d0ae05ea6f8c4cb7407026dee20a434892dbcfb67e80c37939eba5dcf0b5e1a6d879485a595194b64ef2693ff950ebf79751950e9b817e3c93082d8a0a7c4e24514e4	7871b847e0dea3644a330aeec2a7cab867081a971beb5c084dd97f88d1514747ff26477bf11fb15ba2bb0f47a8c16c5d3a5fa7fdf7dbb46e46de83bec068de5abbe8c2e483bb24ed09836a2cdda55dd4e74de2e179eb36ab88c8f35f8e9991013de074b326d4c92e57b7922c69c1087198fcea456b55607e02c2d6c890eb3375	9.37 (1.0702)	190.88 (4.0427)	0 (0)
random noisy RSA-1024	o<oÃ□ÄÅ□Å}L}"3"ß~ß¡n¡™8™–d–£p£›j›–5–¹‰¹ëŠëªE⁸j6j¨v¨ä□äe2eå□åÊ"ËÇ□Ç]&]—b—òŒò‰S‰ddÏlÏxGx}J}□W□¶S¶²N²ÕqÕ°w°ƒƒ˜h¨†P†ò• òX"Xv?v±O±–4–¦r¦zHz™6™…"…ßyßƒOƒÆ‘Æá|áíŒíŒWŒÏm ÏÅŒÅ»†»d4dç†çŠUŠò□òÑoÑœ:œÉ•É¦E¦˜3˜–]–®~®~F~v=v™d™»V»ˆRˆa+aa*aÒmÒÃ_Ã±z±²M²º‡°ÒsÔƒƒÎ•Ì¼Œ¼‡N‡˝`œ7œxFxÔrÕ–a–a1a□9□²M²ï‹ï˝`»U»'1''[ˆË•ÊÆ"Æ□n□p8p¡k¡{H{ÜyÛÀŒÀÔqÕf6fÝ{Ýœkœ›À• À¥s¥• N□‡Q‡°~°Å"Å□X□£l£®~®„P„V&Vd2dg0gè›,èÇcÇŒESŒ…#…ŠUŠ□<□¡k¡Î°ÍÂaÂ□]□{K{²L²•c•d4d–d–ŸlŸj3ja¡à□\□ªuªZ*Z¶• ¶])]^)^…O…ù"ù²□ÊìÊzCz°^°ÌjÌ¬z¬—d—l<lT"TW%WÅ‰ºÅÂ`Â®}®´O´µ…µœhœµRµœiœÙvÛÆ"Æœlœl<lÉ"É',' ƒ˛Ü{Ü³• ³¦B¦¾]¾{J{n6n¾Œ¾Ê"ÊÐkÐ□k□e/eÃ□Ã¤m¤ŠWŠØvØh1h{J{□(□£n£íŠí□+□tDtUU¶†¶•_•Ã^Âœ8œl9lc.c^%^½Š½yByaa|J|—_—□K□´{'‰U‰¹'¹™3™ŠŸŠ□h□\,\□,□Š%Š³• ³è…èÁ□ÁŸhŸÂ'Â‡R‡›d›°}°½Z½"["©w©¼‰¼□M□□.□¿‡¿˜u˜£o££@£"C˝]&]«s«¼Š¼¬t¬‰P‰OO·□·‹Z‹Ç'Ç~N~ÉdÉ%o%‰-L-\&\ÈiÊ÷'÷]-]‰&‰	j8jj1joËgÊî‰½‡½ð□õšhš•d•□l□ä□ä˜7˜'X'RR×s×©t©ô"ô·†·n5nÅ'ÅÂŒÂW'W¸,˛~G~_._™5™"‘,"›7›•4•c2cÓoÓ¡=¡ë…ë‹U‹–b–{B{ë…ë±□±□L□ÈèÈ¸†˛f4fzHz"\"ï˜îxDxÄbÁ¿• ¿TT{G{\%\t>t•)• SS□(□W&Wa(a²,²Æ'Æh7h…Q…ÑoÑ,K,˛□˛'‡¹(Œ\Œ•1•¢¡¢¹S¹ÙsÙó'óí˜ì»„»ºW°ß|ßvBv·T·•'•˜h˜u@u§C§ò□òŠ'ŠÅ"ÅÖuÖ¿†¿ê˜êÇdÇÁ□Á»Z»•)• • \• Y"YÇcÇ–a–õ□õï‰ï-w-÷'÷î□î±N±ó□óÄcÄ□[□…L…¾‰¾ŠRŠ¬K¬À□Å•d•ã}ã}H}ÎiÎØrØ†N†›c›],]□U□"2"r<rú•ú¥B¥±}±²Q²□W□□j□†R†ªzª†N†ÞxÞó□ósšŠÔrÕ½[½„P„e1e'Y'ê…êÉdÉø•ø¥n¥š4§¬H¬»,»À• Å•]□T$T¢>¢·‡·U!U§u§˛„´J,¹W¹ÖsÖ'-'¤@¤ÔrÔ□P□□f□'X'²,²ÉfÉf3f™7™`˛`‡T‡´□´˜r˝ÃŠÃ¢¢<¢'+`□+□º˜ºªI³Â□Â—1—ÙwÙ£m£Â'Â˛,šfšs:sŠUŠh2h¨s˜Þ|Þ□˛□›:›'[˜uDuY)YOO§A§´□´m6m•d•'b'ŸhŸÄ˛Ä˜E˜ö"ö†N†e4e™i™™"‘'á}á¢†èÂ˛ÂŠZŠ• ,• ³R³• \□â~âºV°†S†e1e□˛□¦s|Ÿ{Ý›h›)É'É¡i¡—d—¿Œ¿|C|¢<¢ºU°{D{£@£• g• □□¬{¬ÚxÚ–5–□X□¬w¬n;nê‰ê¿Y¿ÙyÙ□9□‹T‹±□±ŸfŸä□äe/e‹%‹«F«‡Q‡«z«m;m»‡›»8›Z$Z¹ˆ¹	11.52 (0.8602)	192.30 (2.2584)	0 (0)
RSA-2048	a436946b8f2986e00194ffd4e8a609026c9fb664d90438c665da9a5211324ae2eb074ded0d6a733b97c5dbbf2db1345b1c694767c6d81f054dc7837ac62a2abe6610294c7b2637e35854a0b0109ebb0f5ec657533fd9910c8b201eeed024f9e01030bff0e2cde48e797406d625f6c601b24e05ec7c3b94688d9579aefeec8e852189a5c7814dea4a6b597b68a1a308701189d8dc025225af1ded2b35506c92758778d735720e4f3a36814ff323ff0b0f6e8e01a90fd98643d2bd2832c21b54da3da4c4e71ef27585fd165cd2ca7e7d239087ab0b3735d794c3ebc703863f7e144264cedac8da218624476f613da12a9447f3f9a9635c1201fd030bd1e8edc9e6	865da2d6ad34aa610ae0f4ea481ecc47a1f1dd0ff166f6b6521f8d2ddae669c8adfc72132be8268ab76cdfb815563b92c0bb141b9f8f483013cf9bf87a3a5be09359ea627d70a02f56c51ab46cf43a706acdbb0c71a53d4afafbda5a012cd9499c53490929dd2f2ae1683dc188fb6906105282 39eba8f095703a3c00a02d698b82bb4515475995a0ea338c439e106da556b0ab10c5dc900e4f2bc7ae6617b5b30a65e9605e2e56708cf64393b3be7fb433a53fcfab8f555d185abeb1e01905a9af5369765ecd3fac5da04a37e753e8c258fff754a8ccc08daab6b47eb66b94321461141a433fafd3a04909b5e5f2be2022a758691058c176debbfe0b5f58e47d	12.28 (0.8885)	355.21 (0.7506)	0 (0)
random noisy RSA-2048	®}®¢j¢ä˜fäæ…æÁ□Áo;o{J{ê,,êzFzó'óÄaÄ¬t¬ËgËð□ðÄ"Ä,,f6fÙsÙËiË¦m¦ô"ô'/'□N□É"ÉVVâ□â§o§ŸmŸö"ö°x°RRó'ó•_•¿˜¿˜"˜¾Š¾©p©ŠXŠµRµŸ;Ÿ†O†Å□Å□)□´R´©w©ÔrÔyAy¦B¦o:oÌkÌ}H}§t§□O□·„·ç†çœ6œê…êªIª†S†ÃŒÃ¹□¹¼Y¼¿[¿£s£˛ƒ˛˜2˜~J~[$[®L®g2gŠ$Šä~ã□[□SS™i™3Q³Â]ÂÍlÍ²}²~e˜Â•ÂRR©t©□^□œcœ|C|—4—¶□¶,T˛□[□¾‡¾¯w¯Æ"ÆªzªRRœkœw@w□□c3cs=sÂ'Â□«t«}K}ÎiÎìÌ'˛'ÝxÝ¼„¼¬x¬¥D¥i6í´□´Œ&Œ"-"'O'ÝwÝ¿¾]¾±x±□^□©H©d4dÄbÄv=v˜U˜½W½IíŒi¡¡□]□p"Z"»V»QQ~L~›fð□W□'/'ÉcÉ½Š½'/'□*□§C§‰(‰s>s|J|s:suAu¿Œ¿¼Y¼·†·÷"÷ªGªƒƒ¬y¬÷•÷ê˜ê¶¬¶ÍfÎ¶†¶ï'ïy□J□®I®u<uÄbÄó□óxCx®{®˛/˛š8šm6mº„°j1j}G}k6k·□·£k£x@xÒlÒ¢?¢Z*Zê‰êÂ`ÂSS¯□¯‹'‹g5gS#Æ□ÆÂ'Â×v×p>p±}±™6™¶R¶□*□q9q'X'ÃaÃ¢q¢zBz±P±ŸkŸp8p§o§½W½£@£□[□qAqæ„æ«t«q?q¶~¶œjœ©v©•<•¯M¯ÚvÚtAt•N•¡l¡□:□□W□ù•ûn7nªtº©G©ŠWŠc+c‰'‰„,ì‰ïŸkŸ¥r¥~M~"a"†N†ÈfÈ‹U‹……Š&Š˛/˛œ8œ□+□ŸoŸ^&^·R·¶U¶f.fÇ□ÇÔrÔ£qÉ´}'˛˜Ÿ9Ÿ• d• j9j• • —a—®I®b)b·V·{G{¥p¥xDxxAxffᵀᴹ3™□Z□……¡>¡ò'ò□h□©H©Š%Šn5nÅ‰Âé/é£>£œjœ□J□V%Vn:nÞI Þ T$Tv@v´□´"Y'd1d˛□˛›j›İgÌš9šr9r²I²‹Z‹…N…ë‡ë½\½½'½ØuØf3f	18.20 (1.2256)	375.83 (3.3780)	0 (0)

	¥r¥ÛwÜ¡@¡–e– ÚxÚ,L,'\'□,□ÉfÉŒ&ŒzGzà}àzJz±□±šiš □g□Å"ÅÆbÆ¶U¶½†½˜_˜k;k_/_™d™□. • ~L~…R…©v©ÍÍÌ›g›,,•d•¤@¤¢<¢…R… ','ÒpÕzIz¬v¬,□,¶…¶ÙuÛl6l□7□Ã`Ã□\ □½,,½µ□µ«J«~H~q=q©H©¢o¢□\□`0`Å` ÁÖtÖµ□µ`0`o;oö•ö'Y'Yæ,,æT"T–2– c.co:o"2"Š'Š¿\¿„S„ô‹ôÏnÎ™b™²~²-z-•^•yF y§r§'‡'{B{u<u¯y¯°z°¼%¼f1f½…½–F¬, K,ÛzÙr;r*f"ƒ»ƒ»*l3lk7k'X'-x-¼[¼˜d˜¾˜¾X X›8›□)□T!T‡O‡šfš¼„¼¢>¢ÛvÛñ□ñk:k¼ W¼ŸnŸ`*`¡i¡n:nê†êm4m¡=¡[)[• J• • M• Š(Š²N²Ê•È÷˜÷□j□T™6™MÎnÎ%oT%ov¯□:□^, ^³~³|I|à~àÍ"Í□L□†%†Ÿ;ŸƒNƒzCz³N³¥@¥ Æ□Æf4f□7□®L®‡&‡ÑÑÑ§F§%œ&%o|G| ©C©†T†É·ÉŠQŠ|o|¥C¥Å`Å‹%‹ºŠºl9lÆ'Æ Þ}ÞvAv³□³±□±o?oÖpÖ®w®ÛvÛÈ'Ëï%ï □Z□□I□d4d£q£|L|'[']¦B|□W□ã□ã±z±±O ±□<□,,¥u¥ÀŒÀìŚí™f™©s©§C§'.'±L±' Z'q<qWW½[½j5j□]□wBw□L□±P±•e•‹)‹	O²|K|k8kg1g•c•X$X¯ȳ¯µ|µ¡=¡a*ap8pò• ò]+]xAxÊhÊr@rm;mfÎi‰i²z²À]À‡V‡±□ ±Æ• Æ©H©o>owCwXX-I-Ç• ÇyCy°L° n9nV%V—1— Ã□Ãv=v\)\□[□²}²¯y¯ÄbÄÉ"És;s¹S¹Q!Q ½ˆ½%$%k2k□)□□j□d.dò□ò»‹›'‹ïŒï´ P'¦m¦•\•|E|…U…—4— □^□k7k%%R%~¯ˆ¡l¡«x«ÅaÅ¬J¬¯|¯ƒMƒ ÊiÊ~H~é†é,,K,,¶}¶ÉeÉ□k□É"ÉÙuÙà{àr ;r—c— ¥@¥¯z¯÷"÷‹V‹|D||6lr?rrBrvBv• d• ÒqÒ †V†›b›˜e˜½W½‹R‹VVÝ{ÝÍÍ□h□åƒâè† èc+cšgšd3dæ…æ• V• Ã×v×ÄaÄ□P □¶/¶â{à¥?¥X(Xb/b'^'ÀŠÀ‰#‰□.□^V ˆ,I,Í"ÍX"X°□°"‹,"¶†¶X$X–0– ¹U¹' _'xCx,,R,,àzàˆUˆÃ• Ã¿Y¿tCt• d• ¿^ ¿□9□Y#YÀˆÀb0b□9□Ã□ÃyAy□.□š4š —^—{C{ÍjÍßyßªwªdO,ÂaÂ—f— ±|±□(□æƒæÍìÍ|J|{G{'{ˆ6¯wFwÇeÇ®M ®"[“‡%‡vAvi2i»^»³ƒ³ƒKƒ•e•□T□"/"™7 ™□N□ÚwÚÖpÖ˜T˜Ã□Ãß~ßœgœÀˆÀ ÙvÙÛuÛªHª](]%S%‹Z‹Ã‹ÃX!X□;□• • §r§,,R,,¬t¬□[□§u§îŒîÄ^ÃZ%Zßƒßjßjƴ „´_,_j3jµ|µ`)`vCv‹T‹S!S'-'±|±iŠiõ`õi8i			
RSA-4096	60ae9cecba9689ca5772ac7141f5678c96f63 404873b96bacde40a93a50b38cb21acc6379 36be16b64012c9d05eddcba77a92fa52b4d4 dddb0f4cc45b14a3d111ec94a7782e28773e d43ea2b5b05d06411500c889338c90ddf8de d1b8e8f4fc8b961674c7677b6708c34723d6 4978dd7f9eb828ec155db30fd0a020c26d97 cffd239d24e2fd8ade5478dfc3da63727dc54 66ed6e46400ff644112f01312e3c4f1f0746fd 8b42c0e4f29a5841e5d02b396380101813a61 3f107f1c735d23e37a8a3be374248c362d73 eed6fcbee12f4f23123912cafa29c77c69f23 216678ab6f4654d78e1f7df4494562935f0b c352a7c3598ef18c8e5e6221ed515a864224 ab15e7a0d053e341680cefc1bcd792e3482e 98b9650080f9f68fe8635350c683bd064b14 75606e9f753ed5832f70dab9e338e0fec2ac9 f264331962cbef60b5c3a6202acbd9604a9f b6bcfc7a98341d0ad2add7943954580a6158 8cd5be7881faeac7c741a0c78eeec55ae9f4f 6fcdcd64f295ee015cd7f1fb3b56ff680d3c2 155944156cf72e65af1f38bf3575289b9736 1b1d4470a67744e353419dbddafd17392d5 adb448bbaee0a850b2653999b945a1bf7307 6828f3e0f012f7d79d6c7e68ed8748aa6c29 256e73218b5be283f23b42551d0dab23d5b 5da155bd8772694a233ce2a493cf064faf50 99a56ec1f0c975038246daf11964ed7ed3c1 a9824b01ab2	20f384812c1804b4b41f19e851895102b8 9033955d40726f4c3ef67f13a1572edf307 cdc86d2d54100005fb99c1fe9d37af1b3d4 36db5f1c0c5ad5927427936a12ddd32f89 c9297fb77a7e65fc3249bfd349880556c30 04530c672e8264d21a0f7b9149edfddbe8 6221f5c3463a72eaac3d490776c1c0d6cb7 d58a6e3fab8a044a19a3720be7a37b33fd2 05a0b217900542ed60cca2fb0dfe47d92a6 cc51d715563f4950e96cf872107a80c7dfa bc8a150a790fdc2559ff69f7a414dcf095b4 ada21846470a75b279eb110e2b99ba171e a6fc83105046b616310a00de35e4902710 a32e621127242429f219e7baba75f35d65e c8109f0063b849086374b9dd1bebafc569 b27823e403bcfaa9a4693ead29b82f68872 4f3e2cdc833bf156dcc2814dfd721fca19a 08682af19ba97209171f6d7a6a33c5b412 9f8c086a5afc8f68cf50a05c4ee01c1329fe 99d5cf48142236f4b49b93d55ec5e62f3a8 7c651648922949797721e2b2fd92675de6 5d4d542dd4c3802aeea8308eeaff6cf92cd 890bc308d33266773ca076c03ec4b46d5e 0ce007214fba5363ad43ca4ec42faabf895 556e5c1ec816d545b263acaaeffa4e9239e 97a8d0908a2a9f5f5ca0c9cd6be6f225120 7df0faec6e3fe3b342b90a186a81c98d001 2253fef34e22416a69281cecddf4c6a92ee 55d32aa9bc485d016b834732e24aac0a76 5dd9df513f2479517	19.89 (0.9506)	864.21 (6.2761)	0 (0)
random noisy RSA-4096	k;k¾†¼©p©°,°–]– ºY°°Xº‡#‡,…,´O´□F□ÉgÉ:æ,,æÈ'ÈQQŠSŠŠYŠ ½□½µ,µh0hê,,êr@r½Z¼Ä□Äm8m□I• wFw• \ □±L±~H~'.'¼Z¼µPµ□/□¿?¿½Z½Ä□Á~v˜','‹□‹ □(□†T†–1– õ□õ□k□ñ□ñ}G}›h›§n§¥q¥n6nÃaÃ¿‰¿³P³§t§ß| ßá|á¨w¯¹‰¹{D{"'"‹q=q^)^• J• \&\ô□ô□=□‡W‡ □Z□ó'ók4kß{ß«s« > ×q×ÑnÑyFyeeQ!QÉ"ÉOOÉ?£Ä□ÄÊiÊ…L…Ì^Ì ÙsÙÖpÖá}âô□ôw@w~G~"b"ãƒáÅ□Å•b•Å_Ån; nÅaÃ,T,è,è• [• ÞxÞ®}®¿• ¿•]• ¶Q¶X"X{E{□ e□Å_ÅT!T¨T¨¨^%^g5gº„º–f– □H□‰R‰¾‡¼'Z'ÌhÌ{B{ÊéÉvFvS'SÀ`Â^&ˆwF wî□□¿o¿©t©‰S‰†Ut¥Ð¥a1a%W‰`0`□J □□Y□Ç□Ç□O□_* ªsª$4šÛwÛ'ïxî',,'Å□Å'0'ºª×ª „R,,‡R‡Å`ÅvCvÅ‰Å"/"‹©Ð©^%^‹y«®~®d.d«J «·†·Íí¶€¬¶É'ÉŸ=Ým:m½Œ½¦tØtØ´,´□L□«H«Q !Q•]•É'ÈÈeÈV#•Y¶□¶šfš³ÿ³~E~ÉgÉm7m□H□x Bx{C{ò□òU%Uq:q,U,ÐkÐ• • ·‡·‹U‹],]• [• W$ WÅ^Å‡&‡$4šyIy'/'ˆU'ˆ□!ƒƒÅ\ÆæƒæÛwÛ˜Š~¾ Z¾YY¿n¿□O□',û•ûÀŒÀWWœdœ¯¯ñ□ñÇ'Çf .f¼ƒ¼Ê'Êë%œŒÉ+Œ□9□ÛvÛ¿Œ¿Y&Y□M□– a–¯L¯¼Œl¼m5má{á+|+û•û•'•ðŠð"c"—e— ^)^VV£B£%s%ºÅ`ÁÈ□È¼W¼™6™ª„ºð□ô±O ±Å`Å□]□¤>¤□,□‹%‹X#XB–ß°ƒº□(□³Nº□K□³z ³ÛwÛë%œëk8kÌ•Ì_(__+_W&WWWQQ□N□["[q =q,‡,,§B§Å^Âf1fb2b¼„¼ÍƒÍo=oÙsÙ™g™e5e•0• %#%o-G-Å`ÅÃaÃ□j□ç,ç,ÆdÆÃ"Ã'|'»W»— b— ¯u¯ö"ö½‹½¯W¯½½ƒMƒ[$['}'œkœÂ_ÂÎhÎ|L|□□ ÃŠÃ□K□°}°–e– ÊiÊé…éµƒµ¼%¼¶~¶¯K¯á□áµ□µ¯Q¯†O†Ã‹ÃÇ eÇ□□UsÙ□Z□û•ú%%¼ßlÂ'ÂÌhÌ°a"Œ(Œ□□‹ &‹Ç•Ç•'•©E©ó□ôŠXŠWŠWg0gU!UñŒñ³M³®I ®¾†¼,T,□P□'/'†O†©u©«G«‹V‹w?wÃ□Ã□G □,U,□O□ð□ðã~ã,U,v>vÛyÛv?v,M,|p|e0e,N,¼ ‹¼¤A¤R!RX&X¡m¡¯¯|¯§t§ô□óxCx²N²™$™M□=□ ŸkŸ-y-RRë˜êÃ]Á·…·zGzÛyÛl;lÇ'Ç½• ½¼[½ß •õwFwõ□õ¾]¼'0'ˆR´‹W‹Å_ÁT"T‹X‹²L²ŸnŸ«J	-£B£¢p¢ÃŒÃ›c›½…½¥A¥¤o¤ h ~I~'□'□'Â'Â†N†l:l–e– ŒUŒÉfÉ□X□®J®¼[¼Å□À_.¸†ªwª}G}‹%‹T $Tâ}â[#[›d›wFw$8$w?wµPµ°~°¼Y¼,□.zBz'a'§ p§xHxÒlÒ'X'¸†¸o8o,M,´ƒ´ŠQŠ'‰'n=np<pí'iZ &Z□h□ÌgÌÃ□Ã±□±ë…ëƒ"ƒ*ƒY)Yo;o®y®e1ec3e Z%Z´s˜¤m¤r@rŸ%Y¾4‡¾'r´r‰%‹|@|°□°ô'ô§E§¢ =¢□N□X#X½Œ½®y®·ƒ·}F}—f— f0fb/bú•úxFxŠ'Š¯z¯¯z¯l:lg1gœhœ• K• ÎkÎ¿□¿« w«}H}ÖtÖ□:□□V□Æ□Æ~L~ÊhÊÌ"ÌÈnÈ]E}ä □äÅ‹Å²z²ðŠðZ$Z™7™7™¤p¤¾□¼šfšâ~âÂ□Âq8q ÕsÕ□L□˜6˜□.□—2— □<□RR□=□…S…□j□']'—g— ˜B˜¥p¥·□·¡j¡U"Uù•ùœlœb0bi8iU"U©D©ª•ª□[□ í%oíepé¢pé¢ñ□ñw?wÅ%‰ÂÇ'Ç□W□|E|ºO²n<n˜D˜Ôo ÕÇaÇ'ƒ'ƒSQŠŸiŸPPè‡¿é¢fOƒf.f%W%□+□†R†Â _ÅŠ)ŠÅŒEÅœ7œx?x¼Œ½ÆÆ□Æ‹W‹□]□t¡„„q9q †Oº"'\"ÓoÓzBzæ,,æ□Y□¿[¿Ç□Ç"/"|J|n=n™5™ ±y±ÓoÓã□ã‹{‹)(]□\□]*]□I□™g™q8q¢Í•Í³O³□1 □Ç•ÇÝ|Ý'['ú"ú□\• —4— l3l›k›W"W±}±¡q¡˜□k□¼„¼ô"ôé†éwFw□<□□^ □³P³□N□,W,a,a™6™¥ñ¥ô'ô‡S‡œ7œ˜E˜°°QQã □ãÅ]Ån7n½‡½í†ìÁ]ÁŒTŒwDwÅ□Å°ª°N'□ F□ç†ç»ƒ»,N,Ý{Ý°K°³|³U#UÊjÊé/é°ª°©t©f/f□^ □°/°□O□'*'e.e…N…©p©à~âÅŠÅb+b□*□□* • k9k□,□b2bŸkŸ»Z»R"RŠWŠÆc/Æ·…·ß{ßÅ^ ÅÃ□Ã¹…'ô"ô˜ð™ê™ÆbÆ□M□^ˆn6n^%^¡o¡… R…šešõ'õr@rZ*Z‹U‹•d•e2eT"Tq;qç†ç¼'½½Z½ °ç°ÚtÚô'ô0ddddÊeÊâ|â"/"¥s¥'1'‡Ņ"'b"c0c«v«¼ Y¼□P□‰T‰³z³m8mp7p÷'÷']'ÑoÑ•4•,‡¸À•´À [)[ã□ãÃaÃ¾Œ¾ÇeÇ¢k¢µ…µ›c›¬v¬µ~µ›j›±x±~ I~Â]Â'0"t=t'.'±P±□H□wEwl:l°O³□9□Y%Yg5 g¹□'Á□Á□,□i5i"c"µƒµ~J~'¸'U!U•'•â~â[#[s:s›k ,¶□¶"^"ÛuÛ§p§—2— Ÿ:Ÿ-|-ƒ¸ƒ¸ËjË÷•÷õ□ôâ|âÃŒÃÃ"Ä|C|ç†çÇ'Çæ□ æƒSƒ²{²"U"¸,,'èƒéàƒáÇ□Ç¡p¡h1hc/c³□³¹□œ:œ„! „~s~→0•é'é®x®ŕŒĭ'U'"¸"«G«»Z»ƒSƒ³~³‡S‡è,éz Fz□+□~L~·□·‹&‹X(X˜R´¿□¿â□âÅ\ÅÐkÐ"- "'²N²v=vÞyÞËgË□M□¼¼ò□ò™5™k9k^^zFz"	31.87 (1.3718)	881.6271 (6.0158)	0 (0)

«™b™-G-â¦â¦G}g1g˜V˜s<s<ÒnÒWW™4™¯w¯ À□À¼‰¼™6™QQxCx{B{Œ+Œ—3— c2c¾[¾'Y'Â_Ä,‡,,R,˙]'ÐkÐ†Q†Ä“ÁY)Y™c™ ¯D˜À□ÀÎjÎŠVŠ…!…‡"‡ÎkÎ‡O‡ÔpÔ¥ú¥R‹™‰º ÑnÑðŠðÁ'Ám<m•3•Y%Y¡¡?²¥n¥{C{,Q,ÊeÉå• á‡S‡,I,Z)ZÒpÒŸoŸ……])]—b— ´□¯˜,`§s§[([ÚtÚWW¶¬¶‰W‰Z*Z"a"q8q¥p¥Œ YŒ□)□X!X□□¾□¼□n□¯{¯□j□ÓnÒq:q'['l:l ÔrÒŠŽŠðŠðÊjÉU$U±P±Î•Î[+[—1— h5hÃaÂëŠëú"úW%W»Y»‹X‹º‡ºPP□]□â¦â¥o¥ÎkÎ ,N,[#[ÙyÚ□i□ÎkÎ™6™Ã□ÁŽ%ZÊeÊ•/•…#…º Vº\u=uxFxtDtÔtÔg3gi4i¤@¤n=nn6nS"S‡#‡²□²Š XŠ}L}}I}ßyß¯x¯\+\ŒVŒ®H®À□ÂÂ• ÂÂ□Âç …çsCsk9kÍjÍ-K-ɛ=ɛº‰QºSSŸzŸ¯g¯WW‹&‹Ÿ: Ÿ,·,¡>¡ÙsÙàzàµ□µš5šô"ôŠXŠ□[□¥u¥®J®…Q …¯_—3— `.`×t×□=□··ÊeÊyGyg0gvEv¹X¹Ä_ÃŒSŒÉfÉÂ‹ ÃðŸ ð–1– □N□i9i‡Q‡_)_q<q†%†ŒUŒ□W□ºXº a0a□(□ —^— ™7®I®T$TÉfÉ¢?¢ð□ð]&]Ã^Ä¤p¤›d›‹Y‹ŸkŸã □ã• M□™·™ºX^ô"ô±□±q?qzCzÈ"È'1'‡O‡□h □'`‹ÔpÕ¬w¬¼…¼…L…·,·ÙxÙß|ßPP¼…¼±K ±b,b¶¬¶™·™□*□ð□õfÕ˜ðd+d□L□ÔrÔ†$†•4•| q¦º□ºzEz¡=¡¶P¶$bš—e— ^"˜é‡éyAy‡Ry‡Ræb/E…M…□9□µPµÍ"Í˜D˜t:l/Lƒ —3— m4mÑnÑÔpÔ·V·²ª3–ã□m□›6›J,□,□+□U!U½ W½qAqà}àÑkÑ□G□],ƒF"˜V˜ó□ó›9›□:□ŸkŸ£ m£m6m¤@¤Š&ŠªG²²□²®L®È•ÈW&W$cš,,#,,·‡· □e□WWt<t,T¯T¯y¯»…·»…»"/'ã~ãU%U'Z'wFwm<m ¿[¿g/gù"ù¼Œ¼d/d^)^□8□y@y"¯"ÁcÅe/e˜¯˜□K □ÉfÊyCy□Z□³R%%$%ø>ø%%T%—e— • ,□m:m/ÆæÆÃ□ÀÒoÒ•a•×u×á□á©s©ÑoÑÃ` Ã°x°»Ù»ŒSŒf4f‹[‹â□âh1h,R,»Š»yBy¹□'□1□° O°œgœeç,çö"ö□□eœe□g□|E|J•e•ƒJYŸ□,□h5h³ R³ï□Ï,,,,ŸxŸ›d_¶Q¶ŒWŒÁ^Á¥s¥²P²b2b|m|ê†êê ˜ëï□Þ7›'-'p<p‡!‡'+'!WWïŒïâƒâ—g— °~°W□i‡ï"|"‹épɛa+a□,□~Ì~¥q¥¯I¬¶}¶¶□¶r=r[([_/¸³OOɸ<ɛ¹,¹ÙxÙ¯{¯™h™ÊjÊ~3˜dld•3•xA xY%Y„Q„YYè‡èuDul6l½W½ÎhÎ²z³e.e²N²íŠíø•øò □ò□J""0"I‹Z‹b*b½½–d– [([ÐnÐ~F~í7ÆdÆißiã~ãg2g˜X˜¹W¹'R´µTµj7jšgš {C{_(_z³}³)Ôr□Y□Ñl¿‹¿,9›IkÎæ□ɛƒR/□T□g/g ½‹½«I«Á_Á³ÎÊ"ÊÞxÞÙwÙŸwŸ«r«ŧ«K±¤B¤Ÿg Ÿ|I¤@¤£¡£,!,W%WÀŒÃ·,·ó□óQQð• ð'(¹IX¹²N ²Š(ŠUU²{²ÙsÙZ#Z›6›Á}Á'/'›7›r=rVVX'X‡V‡¸ W¸ɛjɛÎmÎtAt□8□k;kÊɛËòŒò…R…i%ïw>wè,,ɛÌ «r«²L²□,□Y%Y^)^¼V¼Á□ÀÂŠÀÔoÔi%ïV$V ô□ô¶†¶yGy])]'Y'‹ó□óò□òÍÍÍ»%»»'Z'—4— ‡W‡ét'é□X□ã□ã¡m¡ð□õ«H«Á□ÃÇ'Ç}L}¡m¡× u×$w§…!…}H}"^"• W• ÉgÉi6i• ^• Y(YÐkÐ¥r ¥Œ[Œ²|²xɛj«Ã·Âi†i…$ɛŠÎfÎ™5™','ä,ä ^"‘[%[—^— µ…µéƒé‘0'¿%«¿‡$‡})]ĮgŸwŸ¡Ã□Ä□J□Ã□Ä‡ %‡"'"—c—Ë•Ëæ,,ætAt§n§u?u–ä– Å"ÅuBu²z²»,»²{²˜c˜Ã"Ã□j□ø•øxBxÛwÛ^- ^ÂcÅÀZÀc/cj1jÞzÞ'X'‹□\□c- cÃ'Ã'\'ÍÍÎ□W□ƒƒ—1— ´„´-H-¡<¡©G©£n£ê‡ê□*□Å_ÅÛtÙ□G□™6™ Á\Á ?t?tU"UWWÄ_Ã](Ĵi‹iš6š°O°ÉhÉí^í¬t–c3c¹…'X(X~E~î□i»…»p?pEdÉ>5›Á'ÂÔtÕp:p´R´ä□âd3d¹ ,¹i6iŒZŒÉÁ'ÁÄ□Áá□â□::□µƒµV"VUU\&\□^□ ®w®ÕpÖ|L|ɛ|ɛ¸_.¸}E}²|²ÂbÁ´,,"b"'|´ÙvÙ˜e˜Ã` Äð□ðÅ•Ä¯p¯,,,,ô'ô³}³¿Y¿™7™½…½ËgË—4— ƒRƒ‹&‹¢+z±‹Z‹}F}□*□□h□"b"Qo8o–f–è‡è– 4–¸R¸–e– »W»·†·å,åi3iq9q]]µ….…µ~J~ú"ü¯G¯²P³s>s¹'¹á~áï □ï†M†ˆX^□:□Z#Zu?u¿Y¿PP¸□¸T!T\'\ÂbÂ•]• -z-³Q³¹S¹ÉcÉã• ä□\□ɛ|ɛ¢†U†ÂŠÀT'"T¡<¡—g— °|°x?xô'ò|p|Ã□Ã¼Œ¼i9ia0aSSh1h£s£|C|ß}ß™e ™ÆbÆŒ'Œ□<□□8□½Œ½³z³^%^□X□|B|k4k² Q²wCw‡T‡¦o|ª§ª□9□^(^Ê•ÊÂdÂªx"ïŒï¸èƒéɛmɛ ·†·ˆW"˜□F□Y$YµQµÂ¸_Âú•ú%%(%ǎ„ǎ[ª[ÆdÆp =p°V°ª†T†ðŒðƒRƒ• W• ÔpÔ˜6˜Z)Zɛɛi†i½¼¥n ¥¸V¸Þ|Þ%ǎ&%ƒƒ¶R¶¯p¯„L„ø"ø×r×ÒrÔÂ^Ã¥B¥ ±N±^%^□[□□7□-z-Æ'Æ¶□¦«H«§t§"d"{F{□ W□¸□¸f3f±□±ÓnÓk5k‹ª‹%¦¡j¡ó• ób/b½• ½¯~ ¯ÆdÆªª|ª|E¦'b'Øv0§q§‡S‡%%X%ɛ£l£¼Z¼QQÃ• Ã…Š…'^'tCt—c—´,´ÙuÙyAy–]– □n□ÙyÙs@s†R†²ª³ª□W□¬z¬j4j□.□Y'YQ!Qr @rÁŒÁRRñ□ñ•^•ð"ðéƒé¬s¬U#Ur<r~I~□Z□í‹í ÆdÆ„„ÙxÙºW°c2cî%ï¾X½ÁŒÃîí‹i¿Z¿ÄbÃW! WÇ□Ç'.'„K„ßyß®J®□M□ö'ödl+dœlœzDzxEx Ã^Â´S´…W¸ª§ª%]¸„S„ª§ª• 9• n=na)aÁ´Å• ;• ¥ C¥$9ƒ!ƒé…ël;l»%»»sAs[&[„„£@£_.¸ã□ã,P,Ùs Ù¼´¾b1bV"V• j• —e— É"ÉW%W°ª°ÔnÒ_V'ð‹ð®K®ë"ëñ• ñ°w°X(XÂ^ ÂŠZŠ□8□ŸjŸ~4~ßyß‹- ‘¼□¼Ê'Êšɛš®{®÷÷"÷ÇfÇ¿Š¿□®v®'¸˙œkœ–f– □P□h8h‹R‹¡?¡'…'‹Y‹ÔmÔk2k𝑓R𝑓«F«ÔpÔzIzˆ U˜l5l{H{ÙwÙë‰ëðŒð™6™f3f'S´sCsr9rZ*Z□ I□□□÷'÷Ê"Ê½Š½Â□Âeeô□ôã,ä®w®Ê'È¿□¿ □\□'.'º∫ºÀ□ÀyDyšaš¹□'yAy½Š½ƒNƒÒpÔ©q© ²L²R˜Â□Âª²z²ÚtÙ¸'¯',ˆÇdÇðŒðî‰ir9r¡}¡µh3h m<m×v×ë‡ëšjš¡p¡ÙÙ'¸'ŒSŒ‡P‡ï˜iS#S• [• Å] Àœeœ€ÛzÛ-H-Á^Á´P´»…»¡m¡ºŠº□i□·ƒ·¬{¬ö•ö □+□ñ□ñ¼„½ÖrÖâ~âð□ð'a'‘'X'•0'¥u¥Š(ŠÈ□Èï «•'•ª©s©É"É˜v˜Á□Á¿‡¿y□U□ï□ïuTµp;p˜F˜" ‰ª±O±ŠXŠÈfÈ]']ø"ø`.`□;¶□¶Ç□Ç□Y□§D§vBv]Ç□Ç'.'³□³zH z£q£ÎnÎ¤□¤yAy□G□ŸnŸl5l5lÁ"Å¿é¿Cz¼□¼É □É½‰½h6h"- “j5jÀ^Àb2b²F²‰#‰X$X[$[t;tðŒðð\$\□V□éƒé□ \□Á□Ám=m¾Y¾Á]Á^"¯¡p¡§E§ÕoÕ™e™M¶C

RSA-8192	483f8d11a82cf07f180dc0e6affcb42e345948283ebbba848165ea286d3d065cc755bdd5a840f7d140e8f27167853bacdd1456e90879308a1c19e7d0ca7c97ff199146f1c5deb7dc68601b4aee7757637e3fd3e9c60d6d7742b72f2b590a06edbe2f040bc7a5f2bba766e7cdb4cce88fab7787f71e6826be8568bdd08e1ed1107e3c2eb258252ab18b743efc5369a60b28b32934c317dc3e2a14dc4b0e17b0f60eefd156b8f6fb0c29b52d884b3fd72ed6cc614a088702a924780ff6f519c63870251e2487e6b343c241844892a8f2ed456cc70bd022e7b6a9e4f021cfd0ddf82a9f0a590518e3ff3b13376f7836fa71ae10129ef462920c32e0fa382fa1770cd450a494021fd15197401fb04a809f8a46f4c5ef3a78f5f9acbde7bf3d6128e272ec8bf3cd475f40b48d7548e579fd09fc1b1617c54a59153d04b9067a96a58dc1fa1348783c92a157ecfc86b2fa0a7835e2b09985943784ddbf304e2fdb220177c305e4a4bfd65d9d060856de4db049630c7b137590d578b984fd5cd7548a7e2a4dc4380dcc4a63edf9945665e50286196e1c91864c37a6a502a03b7ba40bd2ae40660ff91d790dbdc5efa06d015e73a2f7abf8896598c2d9e03929cf1042fb92797afe401b29c5e7f5d2ca0862b52abcec12c994bfddda affd97786801d012c8e2b07a6d7513aaff60a923a48d4837d648e44da15c1357506ae5e184ba2be8f4459563162cffe2a4aed11f33779eec1567afedcace1e4ef7d51dec953bee1867c4f512968b8bafdf7ccc5da16fb60902bd344950c8c16c5741985ad30931dd07bdae2e6b81dfc6e342bd45c3b21b47e39198938e94dc8faa60387d443e73295ce72598381a7310b1dc1e1f45a32bd385edcee32d7c4bc17c19f8c3a597d099b8d819a527b605cb4b0994fa1565271806d5405811dca7413e376238282e1f13cb4596adc542ab7d17eb906d4b1f45502d3a8bce0f412f05bc3c07d7d178ffc0102009f7f8ecbd1648c7fbfa08f5c870c4e53fcd0b85850af6305721b1fba34fd1ec1e369a799a75dbf48f43a5514202c6a0a89c96d234ddf75902ab76540ba549	9ec30f89b56fd70d8a9a64a8d5f65cc30e3413f166ce978a479fddc1f85caae485e7f3c948198fd8870733e21ca1383408a74eafb7802453c423cb8b6e64477801e388c67b3e49e62db9604ec1a61b70d0e882bc2b231c7ad49f5c2a264d1e9ff204933bffb39d93383599d8a24564c9643268a72282e26bd5cc41ab2eb8a71ae1ddc40144c024a704bc5a4c63b56fb63ae0759cffde0be7ac2122b415f0783a312a0fdd810f5c9c599533d120f2eda966090506421187ecd9582d4d2a0e203abd9da4b3b315da046bdf52afa853e10cb051d20617e833e145aff0154900bcb6b849de17967216eb7e28a6d04689416922d466bef9472472505ad857e5fa9095072162b6eab2b7851bc64384f22b39647bc65ed413865709e18e8ddb36da2d6a00c00a96557c91f738ff63bcfc98b7e6257e6442e186fb55290ceb46682b3c08cd08c20ffdbc35ef548166a6460d25dd342a0e11579632a6d9433ba2ed8a09c9ae7ee0de169ed2dbe8313b8f88c9c2c16a7f0af6b9b9953f4e24a594f640ef99a80c0804d8dc5fb71318b4913d31fe78db4a2a85930048ca6e3bcfe950cc32d4cfeeb2e24bc509937201ce19bfb0e3c01ad729c777d1f5afe6290ab8be95925ae59785a2e060eadd8699cd5034dbb40f04f48ef7734e3675ea5b6b86ba668c8cc0667784793d0e47f9018ab1a60106b9173f486d7f64081d46ef55820781753e53f2fb0f83127ce87dc8582d0a0711ef852aa71b17149db93bea0da8d5412812e3d799ac5afab08d077d744fe75688eb478cc0f9ed748dfb046708513704c87f5d0a8df4a6ec28e3202018e940803417590993a72913e7c9a6358a08bfe580bada8e02925b30e33e397821d29683af72b4212f83bebfef8f6177933bc82cc9e2eb5e9640c45aecd7fe9bba45055305c352f61e196184ab98c26ddc3f584d33c1198ceb6dc43fb85acf39288b79ecc547381a734df17b77079ea9a7eeea23db39a963e53c34b372f4b304d8be233d3b3e7eb5cc0cac4b2c9c8c1aeb18c5b12bb7054752d7fcf6f3240c8a10b941e3d7ba9c2ea26f28b403364aeb	35.92 (1.0248)	2625.18 (12.8159)	0 (0)

d1a3d381b633ad187ad7b1f4ac999adab76d79198deff1fcdac6b14349ad078b3c604407bc5ababaab5a6c55534faeeccc4383913c53fa9b6cc8eea9cd4be33e8f06123b9c0e6613f70cb34f3c635478b6086d598279cc3ce1bbf48e6105e710fc98ea0949947be9d1e99c885afdffe784df2d136d40566dcbd8cad55412b8bd744057f1e4e03b109868634b898200136276b78fa06c4d91e713d2eaad28b0c33f73d0a5868fb8b8a8d4b0da6d2e83fa02cd2bc04414c9d1019dec0c8f2e44a3c747e4d51f9410404c58a56edfbc4dba944d525b7b225b4257d63f077d5de5ebe894f814a8a1486216ae7edf8f2b65929531851de3fdcc32181c626585649b

efb774fc0467c809cc9cab54b599144c52dee4a1e77d250294acfb9f28c03c95cf5f4225e87e2ed3528db37a745297a17059a329c4669c8b2bb5858a09a57033b89e2947b46cfdd49ca33161a452ec11236683e9f4181b2c3687192965ff56fdb22846faa01d13234086d97be6d30b71fc98b7f5296556a791dace8465e3137bd035dbee1c7f1381885fe26fb71fe3b8dea24b5b23f52e81b9dbc5127cbe6f36d089182f2ed6fc07373979e37877481354a17488445f23e223cd6dca5d034552c8c92d0e77d03a9b57785e20f6b227ca25f898ab11d5e924cf0d7e81766dcae505e43c7aa9b87cc160f0f02d3a2b584876c5af1442c6866ff0b78c41307f30a97dbf06cb1b

random noisy RSA-8192	58.18 (2.5737)	2636.39 (10.3928)	0 (0)

Average		**24.65 (15.5183)**	**1015.20 (965.7886)**	**0 (0)**

The *RSA-2048* experiments utilized a *public key* as follows:

```
-----BEGIN PUBLIC KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,E03C091242BA1BF3FeCI/5

KgBXgbnQ8T8bV9DIlAUQ7JDah/nKpNJinT5gCpNl9RD/RGP5JA9hTdqaq/GwBrCioaP24tHBDJ2icLDx5qJ
jrDKh4a3B36JeC49PZK6gNTyGy6WdMXCk4h599YYnhVFyWjyPoQTHYgQk2bQkK2/+NAQWkLiDW29V8pr+xh
qGn0rN7oPOkPBSY/XZ5CWb/wstqnTeDB7VmiGPClDBnsYv26bwnpCI5G/iz/okYdgvGlpsOtyTd3P3OYH/4
```

C9/tDraA9UEeACYQ5DsBAmsAncgeY6js+rGz7xS9cyYfYVuqmFrNKABSxtT81TFhzfXjQ2fcROvQOeMNBAK
e/UbQQVXsE1hJ/zynnc9n0KtVGk1AtLGzglzKYCewiB34JQ4D7W/40tK0= -----END PUBLIC KEY-----
'. The *private key* used was: '-----BEGIN RSA PRIVATE KEY----- Proc-Type: 4,ENCRYPTED DEK-
Info:DES-EDE3-CBC,FEA0B6E4A8048D2BJjSA7yUk5aP6oQqi4AOF36ACF0q1oxcpqK5tttPhhl9i5g9X
/wVirndpgs34SP+kElEIqOOBfN4BZtuQnSqkzwOPOzb2Z9VPlCzmCPVKuka9V+lPDKVdoOtpdzAkyK+8PRb
Go3V4ksFUdzhBfaJfdGRBjQ3OEtP4H/i4HygZaSemxnfmxWwgq9ELhHJ+yX8uKtBjn/O50pfKnMQGSZ+pWN
a/dR2nsEkbGueUKYyJeWy+aNAO7O146MUVXFHTW6sMyJNTJs7AHyJ47Ms7Z09Ps7Q7x0S1PHY3XiMb4UyX0
50V3+5c2P9y+2nA9YRhliUi93LIJ6oGhhJhu/VtCkYPSGTau/bu+749gDmN5hUP+U++eHqZ3cxYm9pM1J5i
yFQBBNSq7kuk2O4Uw8iABGPjmoiyckly91udylCqS6FZfqq241fGruR00Q73esSM3QH+wh/IEnFvCOjpUMk
YRSyUHA2XvuFO9zassf3kMv/vqI03qf/6vu4mfwlnfgZigYEIfTUub14wlS82OKieBVtoON8jHXySzrnwmE
5WFANjWKlgRThQRE7K36JhMcIRBk17Xt0e6xRyj/Il5CxB/FDBGBebp8iubbGPEAKEiUMuu4ZwBj5VMpVTS
hcsoMwFS4n4v1qALS+BpZM+FBH5NqoCkW/dE/GHlm16uDd8bSVAODcEOsiB85NaM2UOsU06n2pWv8wdS9yG
8FKqpEJJVDsYka9xtOZ7jA6zRYQIW+OMcyPQW/MkTIj1Sy9+7YeSQSYL6j2tGniTi2d8mn4qOEYY7rimsWE
wqOcx2SnvELZAo8t+rFr/AginnOyHAKhSdHsKC7l42/Gtt4KEyI1viUEOXHD2HtxJ8/mQYJ3om7xBdDAj1F
4bP/Li2ZMuBXHV3gI6z2TZCqjittHC0AmBGMhFuc2PggLWC+wwkXteBB+jpe1ljmdfqOAxekH9zhPSDD5ge
yNOLYbUQag/V1Idppj+wI1noBJeni53Z35V4xrMoMAwMR+RGSu496eYr61sAhpgCnGtR4XKmf7L3XiFCUCn
J0JGGQtKd3QPdmiiW2xpTI2xyvdcFVUL0MEAXyFOMcugfwF+nhwtMxAIynvgKBO5dRK5KknsKiDUsPpBwoa
IdZ9s+BZ5fdYqIjFrk8MjUFsHn1CiMop+BT6fCHjACHjEzZbUhDVrNOSBucxwqnK7b+JAApK9quGjFCyclT
VifIHPAGlONMjhp9f/kWVvh2e09SrCte4jFVKQS7RXwHsBFD/gP0EU7DrfRtqGbqrvmnrGofC5blgBdY8IV
8QFtTG0e+tq/csMURnHsbb+DKF149/Jgz1wE+2myUJXcomi42n8iAynX+I1v/q3XHyo7CmzLjDr8us3pIef
7YB3WoyAcbrjG+cQZlKhQfUXnrQL6M1EGT1n3Dlq1YFJbgiLj6EpC9LYxC4SwKJNoat31yaMWADorwZhjMD
knr64KhaRUSDEF5foVfnyCGZzZ4vT3AjOy0uGBugxrf3DBra1nGA1tK4RbDHlo9njPOAaL5oQIfH5ip39XE
L1rG9gPocxpPhgMRBgmTWMkNYDoRsvG30rly6JjlMCXnUWJg==-----END RSA PRIVATE KEY-----'.

The *RSA-4096 public key* was as follows: '-----BEGIN PUBLIC KEY----- Proc-Type: 4,
ENCRYPTED DEK-Info:DES-EDE3-CBC,F554F9FD0B3A6DE4TAOBqpO7JUvVjCQeKM2
tLuAauvNKGord5RKBFeJvTUOlU81NYUEws+E9qwWoY7Lzm8pigVcHptKyehHW3eb8Xja5jg1lvcBTfJmVfu
Ld7IcbC90k5KA312YGxFEqOsv7ovt156UIJBEnSnvOg8+ngMYLqaOfMjEIcrqLetYh7M+RRQhWq3pkfzt52
daQPnbMBhzWlulTYjW/sKXYDUEHlvB9Iw8yvqJvtBnTEit15SYOeHIXkLZgrF6AbbU88M+jBdZ69rr50Liu
GmWg47S/NWGI01QVAYMdVc8FqrlnVqccequUghXJ+InYkd4pGOH4uEDuUcaLeBiy/DeOszFwuKxN4xrEVpA
YaoKFRQZnTDaUCJ70xjQsWuR9ggboM/1p/iamQhlcI5Ydy4GpjSGVBA5KiYfBHmJH3AuH9L6PePkm3Q/sf/
K+rV9qq9ThQ4rAlxDdAuspBEyrjaPRlpQqha2oQskMt4Gq+Wds028+tAeC+HhRbDGGh/lxYPfpoEafCtmwv
SV0SjMyipnDrRx2K1aHXtZ0vqXXYQttW538w5fB3SiRJCmmquHIyizXUTecPqOZdu50cfJm6ZHg/d8MbMvQ
illsnGKHBJVL6ORJiphvdKR6LhMiojGnWu3ZTep+45yN29w4o4OByrVZZYAL4phEEuvWFmW3pK5vJbOtOTK
e/Rcv0550rKQaWGgXTUrCeH29SnKogGBE2Rlgpe+N9GOaRFva8Vww-----END PUBLIC KEY----- '. The *private key* value was: '-----BEGIN RSA PRIVATE KEY----- Proc-Type: 4,ENCRYPTED DEK-Info:
DES-EDE3-CBC,4542AECD999C8B958CofU3E7o0abzUl8WsEuVzfu1aDUztiAjz//QS1xG+FkP/gbjTBMeZ
hsXUbzF9dRpwS4amews/zeacyZ6FFIJ+093P/HowVZ92bvyPjh525LgPwgZO/HWL6xagaVZmNxt1KkA0npl
umSK1CdkAOOdAgVwBh0tznPiuRPwI+VqDXODs0/KUUcX16kh58sxb0QxEiSmk3dpbBJAZr1xqcWUJnYcRzM
y4OwmcXEZtC2KqEBROdKDG8ZQY8DcfH0caI2789kIr40FGS0PvkMEgbkkhLyZrN+SsxQ3ztKM3Rz0qX+zGy
HOLAkq7LDAd56F6iRPF7DnSYcVybhrLH1uRknSdJmXDrMiPLy30s2F6/FHZxKk7TcdajFog56Dyl7vIdsjx
dLbVnv/cDIMf4Z0hNMUe00vGkFnQAQtW10Gcewm3P6gWECYkWSwHWvVrIPADfgGWN6U74TncgquZjIXHLEY
FNvWOIcgaX9dDSY+1Evc/5Wjdg9yzUqCXjU+bu2gbuTOwxH9VoVRS3uGnnZDfcpaO9RdpVJRC6AiAxcx6A5
EDtOF9QgyKjoTzweINv9LulteUP4CEo+CWsRPMEnIN3RNR+o90olXWdJMqZ8C5OUBw1Ra88S7SvlEWh4U4M
gJxgpyLLkJvYtlJGT1fXQ5aG1k8U6VRvGxzFmfeFeCcTNmu7sG2Gz9JqfrAVusJrFnx/Gk3ZKz6MH0TLPMf
arYKFrdV+ihWrw1NsaV3YcmNXl1y7SJsKp0sPKALZbPw7UT/hTavnwx49N0O4p6yt0k1sJILNDEdnhZlMbG
JoO2A0H5oD///bdKtmzvKj8MtDkfCkcZv9BNr4rT4CPK4ERmkuDhXZY1ulgPUkEC1OUhsElTchR8PWehjSl
9nvJM/IMlcYXSHGEv01f1GNpcJZZjY1Td5q74+k+lEImsRGheZK8jlAEIc5OdggwhByFF2vydzw9JXYso9G
z9hbzt4KCEGx8COPUZbRK9rCiRsYRs1Gb801hqUUooroQsrdPTbQvCPWOG4kpPXRTMFK/8hwDJvVgHOK53n
ZytayZN8hystQd5pL2SGLsFQss0QIeVc4mYhOiUSg+Zu3KE/f8HTsIJk/5YqI5mIQ/TWWfVGHNIm9f3ibaU
ie8BVCPz3VLFDpAzzPpT7bdxK01QI7CrP00n60lDN5AuZKKlYr/XQonL9SnMy3dxylGCsRP7FMUb/LTIGzw
2snyu0Kvqr0ZxoPmpAkCdBdIMneM75hH17nVmfykHgUiiuPosM/dsiqxauMw9WV26gg/lexXn0Fs7rTysQS
6F8a3M5+a61zrBRBBSR5hcPyMA10UJITGJrtLOoa5qNQk6zQ1Bl8PE8dwHor451KMIAb8GFcofzwyAMRKmz
bG+Qx7t8LcnW67LMHiqpw2WXCkrx0SbRW9Npt78unrsqnhcAo3TnT1LjVXQ9zi3r8DEG/gGQr5N0oW3gSAi
xyxURGDb3KLbVXRlXMuTkDa8U7jCTHTWmFcBRUAeB/N4RWz1sd+5DfUDzvxAJkQZeY2BB0V9I1CbyOdQhL2
5QageVqbyvmNvqdHbqMNkQdKKGpgew9/sDO3b1RLdgHqYyp7S8pMPtmnRv2Ervto0XyEJzbnTWGzWGU0wPs
LPlyT6itFHbxgGE8R31B/5F3j8anRGZPFPLjY/Z9fdBCTLBNPVfBrKs13QgRsO+h7tEGeJYmkWU5n4GWYC0
MyWIT3gpFZ2a9ov8u1y+55Pt1vhK8oNKtaWum4+QEW8hLlT6J0icqOZOCPvq7B0qR2u1vY0GelDHOBJH+g/
kqG92H+VlihsaYaNKlQpfYi83mLLJdMXVSHifv743K95vJCovYXDTSP8LNaoKIh3lKTsukM2SeINdw3N2pK
jSCM94toNDid5f7WLLpuTkBxNevpkOfSMqSSwXWjOhu1+f+Et1fYEAE9ALXuNGK579CZDctA6NMPWGiTaKv
GN0Pos+Bhcqr6vFLEcI27pdi5Ngoi/ju8Owswxk+lzudMHtbB/a/ZwCFiFzo1a4DY+xrz1FIUPjpzoatQp8
ujvGJ/e/ahaShgfnhufuuQDHbw0sdYJzbHthJOBr7Odl0b6IsZ5dnOmAD33B5OcEKGOHi4+oCJbAlXa483x
vcmg9h+dFPHbu2TXvPX+p94gmXQyrH6B+xq5jul+kb3iIntARhVzWXoRMAOnu+C9Vzx/FfgkItb/ewA3fUF
ppeSK5hVRWzQ7TZZVaI4/aAVRD+UCpdA9H0shFM2ciSNjMJW9AhGuQqKARwLdEOKsmEs2P8oMknlFthnd5T
zpBjRgaT/HYKLZ+Uc/3BuBnQ7mXNISGujmpPQrrmvGZa+HsTyaDOUPrFS9irnkAjD+tYBER3QFgpHOLAmSR

In+ehmYbnr0W6ambLr6gIuVhRmvMzvFbaa4zxtynD+CP5pa2CzdkwxzcAR3K2N0XJAsw7+UtQNZq7/mfphn
/oV+zLJ7XsbVBgWU8cLaV59osQOlQG/hrtwrMfjq9kQK7/j0qGvnd6YZdC0EYNq6mPVqz08KKDgfSLgrcEm
xyP9d7Mf9JmBTGsDGU/glf1Mlnrqhk/NkIMowP6NG7B/34NTmEse9UAUxp8/3FLqrPwdjH3nLnNfWgDgKjS
QczrrJfoQ7F3iugtLomzkQ8LXfrz9WfSmIknDBY4saxzTahVWfe0PP6a4R5Cl645AckygJHStUI3Xp/TVHq
MpEajS+OHo3ZDwrG3fRYl5YFPli9jzbTNBBpbvob1jc/XnManfTyb1+UqPs2ccSD7L+bEgARPrXyrXpmM6U
VMObYH2o5DRRRn2uiDuTwuxCYuzENPTKjN0JPH4ry+liQWOcyNJIqx5ELleDwTvNjlMjHitX8vQeR6VoDLx
+GEZNwfPRjz5lmm1/Keh4NFEcVU47ZoeKrdWAIFW7c4vCs694LddvvoATdjfJn99eURV36pj1SzNwq4mbnc
ZLgNrro8faY5D6QBWRnzua0JhS6BdbOlCbOGlDjBGY6nQJdfRCIShtFkRY/nI1M0akuuXNEpPx9/TyUGfGc
yXgv8ra/76uPoTlDeBNJl7UdVOvhIvMUVyxuhFaDxw1+ij990NfQafWGn7A1IT7wGgGukwSB5NTS3Zfho17
oqDvDr4ydGE-----END RSA PRIVATE KEY----- '.

The *RSA-8192 public key* was: ' -----BEGIN PUBLIC KEY----- Proc-Type: 4,ENCRYPTED DEK-Info: DES-EDE3-CBC, 2A91A87847915266SjhJFzXyRl3UExM1AMq0Hfa/SNeDrJlGqMd1A
ly9WTF4EjWeHFsbyl+cLCb8Lt7bvW2iamL9Y/fzaOv3eXqXk7gAxbGZ/DnS0Vit4iI9kpoDYvzmCKgg1uRU
6q5zaq5Y6xjEf4lheKO8v7jvbrtW6b5jSLpN5FRuh/DlxgYdi+wYp4He44KLVqepBDlH0z0I/toh8VD0hdw
mwJfC8m8PxV3m5pSUeK0SPGzYnLQ5Dhm9t+Q8yEvMr3XBND/nk4xnasNiKofJQRdhiOo2YB1ZI/mPStLppi
yvlWgjAcx0NxapMtiaCA997jz24ktl87btYQUtdXj6Abl059UoT7WL7O0qn3lacXnS2z9boux1sdrBAGj1h
KaCwS/sP1SHjgByvF5lJ9gitd+s2YiJ+lpUXOm6tXx67m3cEX9Vf/uu8pLo+rNNqHNKFQwelqfIngIsxKb3
I1Cdllk30zWQ9Jz+GacY58zNoNWnReKpiRf2y2E0fH4jYb1qa1tHa7aODc6hY7k/32Frt6U4fQ1dSSxrw3t
0adJvRE+QJomuXME5xaSslZAV9k9EPdCe7lgANLVoSdsdWjjcfvsscPQx/H5P4ESeXdZaly7NwzHEFDLUD2
R+wnJo7YcqaeN2J6pCSEUa9j8SFg+uXYpFsYGb7BCb0li3qhUXXEg81++O7+/ZHSaGr1f0dDuobqYDOXcTW
6ETSJlkIj+mHfZtPz2ZTXT+JnOVWzUVrfmG5N3cMReLI+Y+YS0jGVqPR/nndngj7cVPU+7ChVZjptdkuBPr
tivDj1+FV0x9ketH+9wJwkUq2MmqH7euyIQO7lfoEoY85ijghjTVqzmQzbO6KKqoDugsjPMYBBOUJ9B4nZK
fQtx8AjAd6QaWeT3efVWjxKrtS2y+LWzFUWUvVwzDtf4oXa4Y2r6N8aq7H41whYSudSG+0qh2f2hwYdWGd0
AQ8IS03VInUhZFYWbl3Mfpo3vkbL2UeG7wW3EbESz5kBTPeD765XJoiYDlGmrOCReROIsGplz+whY0zM0Ii
DA73yhC26+FA8Ckrj+InrT8vi0JbDH49Kt+WOclq7CoKxIJQ+B7l9+trqvzcockZsPSJVtejJHiv5Wk5/40
suqSgh8kSP91pNKCGgV2r8oGr5I9rbYfEtcIqa++iJaduWliFZki+eVnoBv+SEbQOfhNGhHWyj1YuU1MRHA
no907oH3230Ey4yVXhSXZuBi4fePBtOTHeAif2Au/nKi1Qu8CRIHka7A280dpQMFBinpSAbYiIsr4puQ69G
7oXLOOFTDg8sayHRk11yz+WdtteukniCbbDYangtYXRvmrgQkVGQpQhzwG8V69LT/91MZ9nxs0cGOLWyddE
Uk0JUeiFgUEDGHGgY8akMbg/92Do/kfxsiZE+Yb66eCXavaw6cQ2tg=-----END PUBLIC KEY----- ' .

Finally, the *private key* was saved as: '-----BEGIN RSA PRIVATE KEY----- Proc-Type: 4, ENCRYPTED DEK-Info: DES-EDE3-CBC, F4D46F10BFF5553D5yaLnRZWcazO
8JUvTasCfUB9HWXKqAK/ve/k8SQfUCfIfEowSqAsSPHf7Iu9B18TzeCnqqDDtR8g4qLQjTk0/jzE8E37Snp
LKt0OHjDehGkSlX82HsuSmbzs7LfXLwgz7z4zoCG/6ZdEPGGXBNAHZ/F1cK0PGWM4N4jEX9lj9g3HW31lXc
aZ8Bk0L1J9scDaO74LY3b8uwvgsalgQvrrVmpFsL4ThCukQKbHrxy5JR6w1AHC4I+qK7eAz8IUyRGmcv0Xd
bRfnWEi1H25EMCDgxCeYGkb6CSRG22XD229PL5bcnZuSs/b337Z+AV/0DOcfQ6ajrT2aYN5StxYYzGyN16E
qC5fEVNEvyt72FmdOMTB6RIgkPnCcUD4xKJYAJh9h1TkICGFWni92V+Xip0iXfYdaDrmcaXoK5v+3Huy4BE
44KjpZGTnNU5/C7botZSvtNmh4mQRPOC1cxn31POWWgDmsrkogHAKkuiuLF4yIuyi02N177isCULnf+PnVq
74h6w6OrXA3ZIZRydMvEF7gPh4rssubXng/YmCXUfh8IvZB0irqDP4r1yZo8lIDRmK5A9nZJOLn+iEon/YK
OSrMd+ZT+J3nEID4W9s/9GtiEYZGFO0hw0cIz+9JB4sEdb+36AoRXvoyLvf1NFhMdz+Wgc/h2DTx57gYNo3
opCeVdRmYKk1Ip4rXS2hjfxc0MG+dJl68HYvh+9Xat73aUQ+l3ym3FNQY3loTOb6U90LQWLrDwV6wPEP3hP
LDKMuujksZycUmPCWn4yxb1Wtj3HmFe2LdYHHqmqEvXDWO0z0xCGQg/x9JyPkhA7SGpQR+9NXKXsQyvQaaz
f7HSI1tauJFbSM8MK87Q34nP7+iHluPp0v1nssEgoQnch7GZByvw5kRkqk5E/Vc2j2s2GzWEFnCgMVfpAOp
I42e0VtWPAoEA/pV8K6XDueL9aiPpIMsMIt8BkqZZymafSqyot0/EzT04IYs3ZmiGmGFibIb8z3zXjNFQvL
gl2X09m71LU0hyBvmWH5c/ltr7/ZddpwRSbigRmg20ibU9dTh7WJMg4MzIRB7wGeKbYYuwntSydP2lMEsPR
3LYZmvE3ewmhAh8HLDC81p6XOptwJqxHxJo/X170T5hMSaWIaGc9Fbsea3ZjpMh8JAH/S4EtCeBVgVNLzNp
BqxFzrao6dybc9iYx5wl4qKO6m85u51wiTYU3oYd1pjJuSvwoj9+Ru/T7AFUtneiNsmSYsAETSU/5KL+Rke
Cx8KE36HSxjTpk8f0LWK5w5pzCJl8j3ijnwX4iBwXAOYGNRfk0V2pZrKZtyhfusWZZa/6QEYM23HX5VFaUJ
fUm7t05dYC1hyg2Nq2f9ViZvr5pCsuxtEMGybbLjQFXJcAMeuZwvlc/ewx0YbWq/jx4K5hzvlhSzBi66btc
yk/s9v6Ln7wIcRaPrq4IHYR7iUugxdRpNn6rDrnDQHLbuHxYkmWa5xe8A70fmwAnraoasM++Pve4vDVHLZH
fN+MYtbd+gb+zazogq54RS3RWriHsyqzeDxR8iOoriTTI6DB8w5K2YU0Rn07fZhRCv4xaxg90RLcT+sNd+/
m/dPhTTEA+jCnMPtfOiWaqTiVcHT6Gf/vHdml29+InQSM1fAadjrxZDK2K9IkbKFwbE1WxdOZsQav0/mjPg
AO4a8x40xx/FNAoX4eZerKb9nrWjilsR6fooK4pYe52a0MzqKWzOH+JVBREKgLZOsdL/jtbhonW3u9pWKY2
QTY8R5fIHRA167QvHcXqmgyLQGUPtLXKNPCEIRDcPlhWR8hkQNiqZ+UkNTs+vuNaRYm+quLrRTKYGvXFou2
lHILXtg/PtuIFT+6EbBbeNkfCGBicmdUk15XUg7Q8CKdpTh9pTIQk7m1LWCdrNzJtCVFnUzz5PaYzXZJBjb
ml6LW9KumhO6nQhYHLSLlQrquS40aIEUuAFWvFMGtMxaMalXS9GAPq57Z0Te6dla570xkmrU7gFP4o0eX+W
MzOw0RnbML1CK6Bz17fXB6z/sZVCx8nxacy9hrwQ3kAiGZCp3bwyEsIrnSUGxYxDZUrUxAxkKgbXb9ArtwL
ZG6EJ810iSZ7aSFNYoy9vFszKyluYI6brHDPYx1XbpUP+dlXC7SDAc57YOQ8oL7LF8zZpGdGQ3m1Pfghsbk
4kYv65TZrS3riBJdzE1KFQ52ZGlhVVNadAIx49WBBNJK1Q7+ubg5EQaAG9f1ZMFPIYK7qdUuf+eIVyPFOST
Rs4sPAjeivJLVM/X8z6i4Du9B8owaPaRk3ABz7A4pqe7g2OpabZ7ZxQxR+0a4zr4MVGCaVxRoGGk9eTj07x
P3IxF4kPB+HzklFaqxQtairl49frGF6Pms4fcOIZkNujyF8uVxIC9My8C0uyJ4HcFT7Pug0LlK9zVsxRqQd
mFgClpXkDUHxiBQyZxem43DXY4SLG/vvVapS1pSOciynAnFB984d0SgIvNCG1U5hJ9ZtPf7dNppO/kgokyT
+5YKFJN1gO0YuyWCyOXpKbb3gcaqbyaMe9hO95ZY8Sh+uXIs++DVqF8KuYk8DUimo6ScM8vUuP9ei4gGik8
kfWjxU+Qk4Kg7lf0PKzvGmPPjELyrj6pf5FOOWqdq6S2n3VuVdXD1WjnStgTW+sgvdl7RqpUR6Baam9KhtK
6mdFaAUZcZvYwxT3BUssZJV6I5j5afLsDzLFpvTQrcI90PKcbTVs6Lv5Tp22tm4rZ9tLv0OB86R6Xsah65h

CJ/gI9bfSs2WAbRextbNfiVY1OWEtHaN4S1o00kS8xnayxbVt8reYH/16LR3Df3OANmp8alEZ5ib1ma8b4Z
2bQLSQ9dxGYXGWwe88UBrGP8+D7XI+WcYzhAPgGOIssmfxpcgKbv+C5d4kbpPX1iAKEwO9HzxeliajF7t1S
lNVUxap9ERPF1AeI90shBjmL2UyHzBbxqpOye1FakTbywBF0vw3TaJbCuMWuB5owX9mIAeab6VH2TogXUlL
72ncOLoLsn+1t+igRlHqDZm7wr6jo3vcT3xDxZez9WD9Vk4Mc5FBrNXBCIkD7YcU28zTQr3z9foSbHlk9TL
wLyTqwYxHN2YwXT/aYlFdvpJ0iaYMnPhcdVsf/HHBYHUitRDlDTi99a8iq03R1PRd+tAZ9tLfVs1A0KVoGn
l7jR1Ow3E7xmEAhlBVT9+fKJXxH+Vlen2KYA1UYakRT4lFN/Y5v2h5qMRWHktuVcofdgX5vadFd1NtTWO4D
wlD+aUgupZUkmVyWqPZInsziTGjcgAQOo2yBz/MvV7yMBwA2IiATyOFv07txVCaAyMeMtUv9YrpyQQWeQ34
8m9UGneaFkhEPH/CEWjHJXz2RFwU44pJ7qqjP9Qu2sDfYuh7zhU5fAP9i1boJGeDP9oKWbUKHS92XG3ZtFD
15bAARgNPcEpARHk9QHMeNKoSoqDHtinHxVK7MCfvI0QYHTjOwlSLlBTk2FvzIfERsi39o3g+nzKipb/j9G
q28E9b+/XhbMpI3yRlplygURJUA0IjesslsJnHJ2zr6OyUD8NnYcJ+bXt2+dvdFtiAuEoMfe/GNRTzfiDvp
SadEL/UIWMjqO8Llb0JgN5eYXeYrMf+cbApCr+aXFcFuRNcFZhjk7dqmaT1aUcfpXTn1fx38hj/pmtxKL1L
TpTztK6IQMmYpbVGBs4UDhNrA5+Wf4KkgNUhXO7KK6SAZfHNkrpddgnzGuyhuDZZwVV6NP+UcqQFW6y0Xda
/m5/57gRUi4qUT+1hgQLXRifsZ50oXhELmCsGbgfCE1mbLWSg3UOoO4o4OBgSo+IyekvIvzu3erWBauL+j6
SgXyyLK789IAuAtpzG+PPT93vx5eNNjuu4JTEwQEaykaaUA36D6yYvVTa355F6Zo7eaSDmOot70B+F3RcgZ
bhOI0RAlA2P2/bMn4W37TgsGE3b1qt5eYkl7HKqTTaw7PA9bgKXMsbZQykW3Nvcb/vT9W+i4yys17HbCK/Z
WrihLeZdWRbwuq2VCg4Mux8dscSGGw56CGBbkO9WrkkL1i/UQx6Gj6T//8n1/BSIWYJsq4qZE7XWvz8Mja9
lNNOyezpxJaTtSZ49npYtr8ko/h20ZejyfgqWPeRG2gJIDXgjRXE1dz2zbr1+Lq0ypryXePblP6/ZT8iBx1
7XLsnBDmLGmO1TcSUCWPRt/qfFMDmK8lZ8BFS3sAUnsBmTWhg9dJDpWMWegUccLQCcuPSkhmFKhsaS81nNx
PR1V9cDJZW7aDbPIbjP5vdEpoZWYQPtMoca/Xms3sscKWbltOGvxye1MLn1unXn1jNEv5wPAB/sDwETwtZ5
u7DetZGVut7aA5tPWVvPUHLjjfDkoEv4hXhVgTkBa3zxUbjznZSWHHZFK16fnDvH9mnIE1DajCAQX3wRtId
vN3rrolTfLgDHg9lwXB4DzUvZRfu7PRdHA5yxMhA5gAOpFtoYzCzbEeLIxtxfIfaGmPQm8IVDFx7AnnFtau
AjVqa7gH6zBqr0b7bqaakh9UrH0IE1A3uO1SWmHytxdytIF1M24iLZLY0QIPLtvN3KqngOPVnTFnLmzy6qV
8tc0zIeVZyLVc9bNnFVtswMLQujEaT43bEncU4r7y3cpeAK9MNI9vqxT/dSAVj/eEO9MCnrUhoVxmw2ujFS
uWHH9iZEfalzUcrnWstAIXslTonwfAhBgkEjLuvIu9sf+1J4uy8ye+jrcgzgmPT9n19kPN/+pg9+5PvZh22
c5pKAEmuRU0DyE45jMGQkE65B6Gl+26T11Ihh8qtFXsYDnFeGiSjTTlviUCeMtuAZhV/1K0FQbDV/SZs5na
OWlqTwN0qKfj22Ho1+9rFTf1CMmSdieICaSi4EbhBeAqx4o7DHjnsfKWP67eOixIqmBuZs1Q9tnDePp5zWK
lpFBGKrn0zswR+68wdMOkuvmwPLj/X6oVlHLH4HhLCrQXIseY3IQooSs1M0dWAHtYgGwqBdr6iQ54a+9Itd
j3dch9lFh3klDZoBU/EvyC99kMOgSzBht19FnF57zN8kzt1vyJ/cHbvOlrtIrYT2OijI+u4yazNFpGwnj54
bV0ZstAkv0wwPlCdhoP9vQ5mAmi1IbQmLP0akkCEI0hW0GlvKpW83Zrxdj8CNVp4wcFM1QkJ7mHHIMG2iX2
u81DBCXN+c9jSOwfPh5/1MpA2SpmWm5vqyR4qSRS+08SoThVOdTgT6F+e45bEHHNw+iO46wdOezPTPU0NpD
uGDO6ewqPU+ABHNh8T85kNni+WamqPGBVMHGvw+j4LVsnBjPRiw/xi7W1dwgVZsndWwLPvNVQ4ytc0CdIv8
dQj9EVQs9r6JnSt3+imxo8wBRYMRqgXOxsHOEnEhVPvelVxM7sxZr9uT3YBHdlrq5AS2u/3dThGsghkSwsT
e1b2/huOc/Dh9/dp52BIFCF4BCQDI718a4W/fjgQybxjsWGYLHZO9gI6dbVk9gUPf6jLhj2ygIGI0csKXsW
eNPtRNKYyPEQSZdQsgyCIClEzUDgs079r5v86rnEQ8RnVJfbkW5Ii3xmIGEeUx7H2rGvH/Ab+WAp0FqrxFy
llYrxGmufk0u1ijVE/mvk75dfSRXhxPKDALBIDWpaAYbkP1O3hPHbHgPT+Cs0WWGQNned40TqpLwK6X4Wmh
v+avoRQ6qmyXvrfHQ7nZJjrYhwVBhpjIVa/tnQdXex9Zx10HR6bhwao8UXiMsY4ODJpNyvKaJnPb/RmauxT
WJoR5i5KvenC7YIJ2k4grEq+k9+qGPtsK+yTL5PjylQYnRVMz2nxjnNTJjPTrbvgihrl3WXMIsjoi/dJCmc
FHADagq0FgGc6KQ6GwMv7sVvrNsAx1h46qQl3EMMdnUTR22ldwCFTsfRybiWqKU+rYS+FMGNmmpkpsdPljb
42idX+7RD1dAX2HlJ8qYFePNCUdRV5WJ1kLC/suRiLl9FuR/nZ6CfCjXtHeRuFw+FFrDLCFXfUNbizlJ0sW
XcorZSGaXaB2tDZr8cc14eelcUjEt0PcDiKieA00jaYdPJp4civaapcWS6T8OBaznJI8Ich5RUOZpjwtSHP
IZSHW9hLH1tQfEtKSlEaglLzvta+mQfQlOjgRBH91NYk3495KYwtqCiK5/YGUdY61nNkWN6fC0KhDyHRgUP
Bv5C2HkxW3OOVlr/gsLhNfpAyoYOt1aPc2HnirT7w1iEF0FLtNOCHK -----END RSA PRIVATE KEY-----
-'.

These RSA keys were created with pycryptodome (PyCryptodome 2025; PyPI 2024). The calculation of *encryption/decryption times* (ms) and *estimated error* are shown in Table1. The *random noisy* strategies generate *dynamic* and random results, always producing different outputs. *TC* and *TD* are *average* times of the estimated procedure for *encryption* and *decryption* tasks, respectively, with *standard deviation* in parentheses. Two *tests* with the same *plaintext* '▒Welcome▒?' show different results. According to (Rangel et al. 2025a), a challenge of *random noisy* approaches is that there is no control over the chosen maximum *ASCII* random value. Using *mod 120* avoids invalid *ASCII* values.

The *RSA-1024* standard variant was definitely the fastest for encryption, being 1.23 to 6.21 times faster than the other strategies analyzed, with a range of 2.15 to 48.81 milliseconds. However, *RSA-1024* may be more vulnerable to cyberattacks compared to the other variants. This is not the case with its *noisy random* version, which has a *double dynamic* security scheme. Moreover, the *random noisy strategies* improve data security (Rangel and Rangel 2024a, 2024b; Rangel et al. 2023, 2025a, 2025g). *Table 1* compares standard algorithms with *noisy injection*. Regarding data decryption, the process was slower in all cases. The *FinalPackage* processing time was longer than standard algorithms (see *Table 1*). The speed comparison for data encryption between the *standard RSA* version and its *noisy random variant* is not substantial, ranging from 2.15 to 22.26 milliseconds. Similarly, the comparison of decryption techniques ranges from 1.42 to 11.21 milliseconds, which is not very significant. Despite that the 255-character limitation did not affect experiments but suggests further analysis.

All *random noisy* schemes produce *dynamic* output but make decryption more challenging without the K_i value. According to (Rangel et al. 2025a), a *PartialNoisy* proposal increases security digital data. *Noisy injection* protects against *cyberattacks* (Baklaga 2024; Bavdekar et al. 2023; Iavich et al. 2024; Rangel et al. 2025c). The *random noisy* alternatives can reduce data theft risk by inserting noise into the *ciphertext*. The *noisy injection* proposal with *RSA* produces *double dynamic* outputs, confusing attackers (see *Table 1*). *RSA* with *random noisy* show promise for organizations seeking security. The *random noisy* scheme is recommended to enhance digital data security in *RSA* schemes. *Noisy injection* ensures significant security improvement.

Other techniques like *reduced noisy* (Rangel et al. 2025a) and *reduced random mutation* (Rangel and Rangel 2024a, 2025g) can reduce *ciphertext* size in *FinalPackage* by 33%. Another strategy is applying different *noisy injection* methods, like combining *random noisy* with *artificial intelligence* using *nearest neighbor* rule (Barandela et al. 2003; Cover and Hart 1967; Rangel 2002, 2022; Rangel et al. 2023, 2024, 2025c; Rangel and Rangel, 2024b) and *pseudo-hexadecimal* (Rangel et al. 2023, 2024, 2025c). This suggests several directions for future work.

CONCLUSIONS AND FUTURE WORKS

Updating cybersecurity strategies is crucial but doesn't guarantee total security. Vulnerable *encryption methods* are a problem (Rangel and Rangel 2024a; Rangel et al. 2025c). *Dynamic encryption* alternatives are recommended to combat digital data theft (Rangel and Rangel 2024a, 2024b, 2025a; Rangel et al. 2023, 2024, 2025a, 2025b, 2025c, 2025d). This article compares *standard asymmetric RSA encryption* algorithm and presents *random noisy RSA variants*. These variants use *random Caesar II mod 120* and have potential for practical application in organizations. The approaches employ *noisy injection* with *random* and *heuristic* techniques, such as *GA*, thereby justifying the use of *AI*. The *noisy injection* methodology can increase the utility and applicability of *standard encryption* methods. Experimental results with *random noisy* confirmed its ability to handle cyber attacks and data security. Future studies will explore techniques to reduce *ciphertext* size with *reduced noisy schemes* (Rangel et al. 2025a), and *reduced random mutation* (Rangel and Rangel 2024a, 2025g). Another approach is applying different ways to achieve *noisy injection*, like combining *random noisy* with *artificial intelligence* using *nearest neighbor* rule and *pseudo-hexadecimal* encoding. This opens several possibilities for future studies.

ACKNOWLEDGMENTS

This work received partial funding from the Tecnológico Nacional de México (TecNM), I.T. Ciudad Altamirano campus.

REFERENCES

1. Delman, B. 2004. "Genetic Algorithms in Cryptography". M.S. thesis [Thesis for the Degree of Master of Science in Computer Engineering], Department of Computer Engineering, Rochester Institute of Technology, RIT Scholar Works, Rochester, New York.(https://scholar.google.com.mx/scholar_url?url=https://repository.rit.edu/cgi/viewcontent.cgi%3Farticle%3D6460%26context%3Dtheses&hl=es&sa=X&ei=cbaZZoadNt246rQPnd604AU&scisig=AFWwaeaMfCM5ORUFQN6DU4LA3aEG&oi=scholarr, 23/03/2024).
2. Kalsi, S., Kaur, H., and Chang, V. 2018. "DNA Cryptography and Deep Learning using Genetic Algorithm with NW algorithm for Key Generation", Convergence of Deep Machine Learning and Nature Inspired Computing Paradigms for Medical Informatics, Image and Signal Processing, in Journal of Medical Systems, [e-ISSN: 1573-689X], vol. 42, no. 17, december. DOI: https://doi.org/10.1007/s10916-017-0851-z.
3. Mendoza, J.C. 2008. "Demostración De Cifrado Simetrico Y Asimétrico", [Universidad Politécnica Salesian. Cuenca, Ecuador. ISSN: 1390-650X], Ingenius, Revista de Ciencia y

Tecnología, núm. 3, pp. 46-53. (http://www.redalyc.org/articulo.oa?id=505554806007, 09/11/2024).

4. Rangel, E., and Rangel, K.U. 2024. "Novel Random Encryption Methods Based On Mutation Strategies Of Artificial Intelligence", SPCSJ: Scientific and Practical Cyber Security Journal [Published by Scientific Cyber Security Association in Tbilisi, Georgia], ISSN: 2587-4667, vol. 8, no. 3, pp. 84-91, september issue. (https://journal.scsa.ge/ issue/september-2024/, 05/11/2024).
5. Rangel, E., and Rangel, K.U. 2025a. "Mejorando la seguridad del algoritmo Camellia, mediante la inyección de ruido sobre textos cifrados utilizando procesos basados en inteligencia artificial", INTELETICA. Revista de Inteligencia Artificial, Ética y Sociedad (Edited & Published by IBERAMIA, Iberoamerican Society of Artificial Intelligence: Sociedad Iberoamericana de Inteligencia Artificial in Valencia, España). ISSN: 3020-7444, vol. 2, no. 4, pp. 75-101, september 2025. DOI: https://doi.org/10.4114/INTELETICA.vol2iss4pp75-101. URI: https://inteletica.iberamia.org/index.php/ journal/issue/view/4, (https://inteletica.iberamia.org/index.php/journal/article/view/45, 03/09/2025).
6. Rangel, E., Rangel, K.U., and González, L. 2025a. "Dynamic Encryption Methods Based On Noisy Injection And Camouflaging Ciphertext Strategies With Artificial Intelligence". SPCSJ, Scientific and Practical Cyber Security Journal [Published by Scientific Cyber Security Association in Tbilisi, Georgia, ISSN: 2587–4667], vol. 9, no. 1, pp. 82-104, march issue. (https://journal.scsa.ge/papers/dynamic-encryption-methods-based-on-noisy-injection-and-camouflaging-ciphertext-strategies-with-artificial-intelligence/, 23/04/2025).
7. Rangel, E., Rangel, K.U., and González, L. 2025b. "Inyección De Ruido Para Encriptado De Datos Dinámico Con Inteligencia Artificial. Caso De Estudio: Algoritmo GOST R 34.12-2015", Revista Electrónica de Divulgación de la Investigación del SABES (Revista de la Universidad del SABES. Editada por Sistema Avanzado de Bachillerato y Educación Superior en el Estado de Guanajuato. México). ISSN: 2007-3542, vol. 29, pp. 11-36, edición junio 2025. https://sabes.edu.mx/revista-electronica/28/# , (https://sabes.edu.mx/revista-electronica/28/docs/2_inyeccion_de_ruido.pdf, 01/08/2025).
8. Rangel, E., Rangel, K.U., González, L., Ortiz, A., and Rodríguez, C.A. 2025c. "Four Dynamic Encryption Alternatives With Artificial Intelligence Based On Pseudo-Hexadecimal Noisy Injection Schema For Handling The Theft Of Digital Data Problem", SPCSJ, Scientific and Practical Cyber Security Journal [Edited by SCSA - SPCSJ - BOAI, Published by Scientific Cyber Security Association in Tbilisi, Georgia, e-ISSN: 2587-4667], vol. 9, no. 3, pp. 59-77, june. https://journal.scsa.ge/issue/june-2025/, (https://journal.scsa.ge/papers/four-dynamic-encryption-alternatives-with-artificial-intelligence-based-on-pseudo-hexadecimal-noisy-injection-schema-for-handling-the-theft-of-digital-data-problem/, 27/07/2025).
9. Rangel, E., Rangel, K.U., Medrano, J., Bernal, C.A., and González, L. 2023. "Algoritmo Genético Para Cifrado De Datos, Basado En Un Nuevo Concepto Pseudo-Hexadecimal Con Inteligencia Artificial", Tecnológico Nacional De México, Instituto Tecnológico de Ciudad Altamirano, Sexto (VI) Congreso Nacional De Investigación En Ciencia E Innovación De Tecnologías Productivas, Cd. Altamirano, Estado De Guerrero, México. Noviembre. (https://www.cdaltamirano.tecnm.mx/index.php/17-vi-congreso-nacional-de-investigacion-en-ciencia-e-innovacion-de-tecnologias-productivas/140-tecnm-40, 23/03/2024).
10. Rangel, E., and Rangel, K.U. 2024b. "La Regla Del Vecino Más Cercano Como Alternativa Para Inyectar Ruido A Mensajes Encriptados Por El Algoritmo: Noised Random Hexadecimal", INTELETICA. Revista de Inteligencia Artificial, Ética y Sociedad (Edited & Published by IBERAMIA. Iberoamerican Society of Artificial Intelligence: Sociedad Iberoamericana de Inteligencia Artificial in Valencia, España). ISSN: 3020-7444, vol. 1, no. 2, pp. 1–15, december issue 2024. DOI: https://doi.org/10.4114/INTELETICA.vol1iss2pp1-15. URI: https://inteletica.iberamia.org/index.php/journal/article/view/16, (16/12/2024).
11. Rangel, E., Rangel, K.U., and González, L. 2024. "Cifrado De Datos Dinámico Con Inteligencia Artificial, Utilizando El Nuevo Formato Pseudo-Hexadecimal", Revista Electrónica de Divulgación de la Investigación del SABES (Revista de la Universidad del SABES. Editada por Sistema Avanzado de Bachillerato y Educación Superior en el Estado de Guanajuato. México). ISSN: 2007-3542, vol. 28, pp. 46-73, edición diciembre 2024. https://sabes.edu.mx/revista-

electronica/27/# , (https://sabes.edu.mx/revista-electronica/27/docs/4_Cifrado%20de_Datos_Dinamico.pdf, 17/12/2024).

12. Barranco, F., and Galindo, C. 2022. "Criptografía básica y algunas aplicaciones". Universidad Jaume I, Departamento de Matemáticas, Castellón, España, octubre. URI: http://hdl.handle.net/10234/ 201359, (https://repositori.uji.es/items/35da2f29-ee4a-4dbc-a82f-c450a81cf9be,13/04/2025).
13. Baklaga, L. 2024. "Leading The Way In Quantum-Resistant Cryptography For Everyday Safety". SPCSJ, Scientific and Practical Cyber Security Journal [Scientific Cyber Security Association (SCSA).Tbilisi, Georgia, ISSN: 2587-4667], vol. 8, no. 3, pp 65-73, issue. (https://journal.scsa.ge/papers/leading-the-way-in-quantum-resistant-cryptography-for-everyday-safety/, 23/03/2025).
14. Bavdekar, R., Eashan-Jayant, C., Ankit, A., and Tiwari, K. 2023. "Post Quantum Cryptography: A Review of Techniques, Challenges, and Standardizations", In 2023 International Conference on Information Networking (ICOIN).
15. Dhany, H.W., Izhari, F., Fahmi, H., Tulus, M., and Sutarman, M. 2018. "Encryption and Decryption using Password Based Encryption, MD5, and DES", Published by Atlantis Press, [ISSN: 2352-5398. Open Access: CC BY-NC], license: http://creativecommons.org/licenses/by-nc/4.0/.
16. Gómez, S., Arias, J.D., and Agudelo, D. 2012. "Cripto-Análisis Sobre Métodos Clásicos De Cifrado". Scientia Et Technica, [Universidad Tecnológica de Pereira Pereira, Colombia, ISSN: 0122-1701, Año: XVII], vol. 2, no. 50, pp. 97-102, abril, DOI: https://doi.org/10.22517/23447214.6681, (https://revistas.utp.edu.co/index.php/revistaciencia/article/view/6681, 16/04/2025).
17. Kumar, A., and Sharma, S. 2021. "A Study on Historical Cryptographic Techniques: Caesar Cipher to DES", International Journal of Advanced Science and Technology, 30(2), pp. 555-564.
18. Rodríguez, J. 2020. "Operadores Genéticos Aplicados A La Criptografía Simétrica", [Proyecto De Grado], Universidad Distrital Francisco José De Caldas. Facultad De Ingeniería. Ingeniería De Sistemas. Bogotá, Colombia. (https://repository.udistrital.edu.co/ handle/11349/28192, 06/05/2024).
19. Van, H.C., and Jajodia, S. 2011. "Encyclopedia Of Cryptography And Security". Springer Science & Business Media, [ISBN: 978-14419-5907-2], 1416p.
20. Van-Tilborg, H.C.A. 2005. "Encyclopedia Of Cryptography And Security", TUE Research portal. Springer, pp. 114-115, 201-202. DOI: https://doi.org/10.1007/0-387-23483-7, (09/11/2024).
21. Courtois, N.T. 2012. "Security Evaluation Of GOST 28147-89", In: View Of International Standardisation. Cryptologia, Vol. 36, no. 1, pp. 2-13.
22. Dunkelman, O., Keller, N., and Weizmann, A. 2023. "Practical-Time Related-Key Attack on GOST with Secret S-boxes", In: Handschuh, H., Lysyanskaya, A. (eds) Advances in Cryptology - CRYPTO 2023. Lecture Notes in Computer Science (Annual International Cryptology Conference. Publisher by Springer, Cham., eBook Packages: Computer Science R0), ISBN: 978-3-031-38547-6, e-ISBN: 978-3-031-38548-3, vol. 14083, no. 1, pp. 177-208, august. Available at: https://doi.org/10.1007/978-3-031-38548-3_7
23. Fulgueira, M., Hernández, OA., and Henry, V. 2015. "Paralelización Del Algoritmo Criptográfico GOST Empleando El Paradigma De Memoria Compartida", Lámpsakos, núm. 14, pp. 18-24. Fundación Universitaria Luis Amigó Medellín, Colombia. E-ISSN: 2145-4086; july-december. http://dx.doi.org/10.21501/21454086.1633.
24. Ishchukova, E., Maro, E., & Pristalov, P. 2020. "Algebraic Analysis of a Simplified Encryption Algorithm GOST R 34.12-2015", Computation, 8(2), 51. https://doi.org/10.3390/computation8020051.
25. Gundaram, P.K. 2024. "Algebraic Cryptanalysis of Reduced-Round International Data Encryption Algorithm", Research Square, ISSN: 2693-5015 (online), PREPRINT (Version 1), august. https://doi.org/10.21203/rs.3.rs-4785692/v1.
26. Daemen, J., and Rijmen, V. 2002. "The Design of Rijndael: AES - The Advanced Encryption Standard". Springer. DOI:10.1007/978-3-662-04722-4, (23/03/2025).

27. Rahman, M.S., and Hossain, M.S. 2021. "A Secure Private Key Cryptography Scheme Using RSA and AES". Journal of Cybersecurity, 1(1), pp. 1-9.
28. Saini, A., Tsokanos, A., and Kirner, R. 2023. "CryptoQNRG: a new framework for evaluation of cryptographic strength in quantum and pseudorandom number generation for key-scheduling algorithms", The Journal of Supercomputing (e-ISSN: 1573-0484), vol. 79, pp. 12219–12237, july, doi: https://doi.org/10.1007/s11227-023-05115-4. Available at: (https://link.springer.com/article/10.1007/s11227-023-05115-4, 14/04/2025).
29. Progress Software Corporation, Telerik. 2022. "Cifrado Y Transferencia De Archivos: Los Mejores Cifrados Seguros Para La Transferencia De Archivos", Ipswitch Blogs (2020-2022). Available at: (https://ipswitch.com/amp/es/los-mejores-cifrados-seguros-para-la-transferencia-de-archivos/, 31-08-2024).
30. Álvarez, D. 2019. "Algunos Aspectos Jurídicos Del Cifrado De Comunicaciones", Derecho PUCP [Pontificia Universidad Católica del Perú], núm. 83, 2019, pp. 241-264. DOI: https://doi.org/10.18800/derechopucp.201902.008, (http://www.redalyc.org/articulo.oa?id=533662765008, 09/11/2024).
31. Nagaraj, S., and Srinadth, V. 2015. "Data Encryption and Authetication Using Public Key Approach", International Conference on Computer, Communication and Convergence (ICCC 2015).
32. Oppliger, R. 2005. "Contemporary cryptography", 1ra. ed., Artech House Computer Security Library, [Boston/London, ISBN: 1-58053-642-5, 978-8189265038], 510p. (https://www.google.com/ url?sa=t&source=web&rct=j&opi=89978449&url=https://theswissbay.ch/pdf/Gentoomen%2520Library/Cryptography/Contemporary%2520Cryptography%2520-%2520Rolf%2520Oppliger.pdf&ved= 2ahUKEwiT1tm1xNWMAxUAmO4BHWYLNa0QFnoECBoQAQ&usg=AOvVaw3GvxLI6QzJhvEXqcl9efPz, 13/04/2025).
33. Stinson, D.R. and Paterson, M.B. 2019. "Cryptography: Theory and Practice", (4ta ed.). Chapman and Hall Book/CRC Press [Taylor & Francis Group, ISBN: 978-1-1381-9701-5]. (https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.ic.unicamp.br/~rdahab/cursos/mo421-mc889/Welcome_files/Stinson-Paterson_CryptographyTheoryAndPractice-CRC% 2520Press%2520%25282019%2529.pdf&ved=2ahUKEwi8_euUtdWMAxWzh-4BHShGAaQQFnoECCUQ AQ&usg=AOv Vaw1DCBGkDbaZMeHuyR45xZZC, 13/04/2025).
34. Muhammed, R.K., Aziz, R.R., Hassan, A.A., Aladdin, A.M., Saydah, S.J., Rashid, T.A., and Hassan, B.A. 2024. "Comparative Analysis of AES, Blowfish, Twofish, Salsa20, and ChaCha20 for Image Encryption", Kurdistan Journal of Applied Research (Published by Sulaimani Polytechnic University, ISSN: 2411-7684), vol. 9, no. 1, pp. 52–65, may issue, doi: https://doi.org/10.24017/science.2024.1.5, URL: https://doi.org/10.48550/arXiv.2407.16274. Available at: (https://arxiv.org/abs/2407.16274, 01/06/2025).
35. NIST. 2001. "FIPS PUB 197: Advanced Encryption Standard (AES)", U.S. Department of Commerce.
36. Singh, P., and Kumar, P. 2022. "Optical encryption using fractional Fourier transform and spiral phase plate". Optics Communications, 503, 127629.
37. Schneier, B. 1994. "Description of a new variable-length key, 64-bit block cipher (Blowfish)", In Fast Software Encryption.
38. Schneier, B. 2000. "Secrets and lies: Digital security in a networked world". Wiley.
39. AL-Maqtari, E.A., and AL-Maqtari, E.A. 2024. "Performance Evaluation for AES, Blowfish, DES, and 3DES Cryptography Algorithms", PUIRP: Partners Universal Innovative Research Publication (ISSN: 3048-586X, Tamilnadu, India), vol. 2, no. 5, pp. 86-95, october, doi: https://doi.org/10.5281/zenodo.13974870. Available at: (https://www.puirp.com/index.php/research/article/view/81, 27/04/2025).
40. Rangel, E., Rangel, K.U., González, L., Bernal, C.A., Ascencio, L.J., Reynoso, R.I., and Rodríguez, C.A. 2025d. "Novel Dynamic CAST-128 Encryption Scheme And Comparison With Five Random Noisy Injection Strategies With Artificial Intelligence", SPCSJ, Scientific and

Practical Cyber Security Journal (Edited & Published by SCSA, Scientific Cyber Security Association in Tbilisi, Georgia). ISSN: 2587-4667, vol. 9, no. 4, pp. 32-49, september issue 2025. https://journal.scsa.ge/issue/september-2025/, (https://journal.scsa.ge/papers/novel-dynamic-cast-128-encryption-scheme-and-comparison-with-five-random-noisy-injection-strategies-with-artificial-intelligence/, 13/10/2025).

41. Wang, S., Cui, T., Wang, M. 2016. "Improved Differential Cryptanalysis of CAST-128 and CAST-256", In Information Security and Cryptology. Inscrypt. Lecture Notes in Computer Science [Chen, K., Lin, D., Yung, M. (eds), Springer, Cham, ISBN: 978-3-319-54705-3], vol 10143, march, 2017, doi: https://doi.org/10.1007/978-3-319-54705-3_2. (https://link.springer.com/chapter/10.1007/978-3-319-54705-3_2, 01/07/2025).
42. Aoki, K., Ichikawa, T., Kanda, M., Matsui, M., Moriai, S., Nakajima, J., and Tokita, T. 2000. "Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms—Design and Analysis", Proceedings of the Seventh Annual Workshop on Selected Areas in Cryptography (SAC 2000), Springer-Verlag, LNCS vol. 2012, August Issue, eds. D.R. Stinson and S.E. Tavares. Springer-Verlag, Berlin, pp. 39–56.
43. Sami-Sulaiman, A., and M. Hammood, M. 2025. "Enhancing AES Security based on Camellia Key Schedule", Samarra Journal of Pure and Applied Science (e-ISSN: 2789-6838), 7(1), march issue, pp. 299–309. DOI: https://doi.org/10.54153/sjpas.2025.v7i1.1020. Available at: (https://sjpas.com/index.php/sjpas/article/view/1020/400, 30/03/2025).
44. Garai, H. K., and Dey, S. 2024. "A multi-step key recovery attack on reduced round Salsa and ChaCha", Cryptologia, vol. 49, no. 3, pp. 252–267, Jun. 3, doi: 10.1080/01611194.2024.2342918.
45. Rangel, E., Rangel, K.U., Bernal, C.A., González, L., Rodríguez, C.A., Ascencio, L.J., and Reynoso, R.I. 2025e. "A Case Study of the Salsa20 Encryption Algorithm Using Random Noisy Injection Enhanced by Artificial Intelligence", Revista Innovación y Software (Innovation and Software Journal. Revista de la Facultad de Ingenierías y Arquitectura de ULASALLE. Editado por: La Salle Universidad, Arequipa, Perú. ISSN: 2708-0927, ISSN-e: 2708-0935), vol. 6, no. 2, pp. 134-158, Mes Septiembre - Febrero, 2025. DOI: https://doi.org/10.48168/innosoft.s24.a317. URI: https://revistas.ulasalle.edu.pe/innosoft/issue/view/24. URL: (https://revistas.ulasalle.edu.pe/innosoft/article/view/317, 30/09/2025). Available at:https://revistas.ulasalle.edu.pe/innosoft/article/view/317/413, (07/03/2026).
46. Rangel, E., Rangel, K.U., González, L., Bernal, C.A., Rangel, C.M., Reynoso, R.I., Rodríguez, C.A., and Ascencio, L.J. 2025f. "ChaCha20 Encryption Algorithm Security Enhancement through Artificial Intelligence-Based Random Noisy Injection: A Case Study", CULCYT. Cultura Científica y Tecnológica. Revista de investigación en ingeniería e innovación tecnológica (Editado por Revistas Electrónicas, Universidad de Ciudad Juárez, Chihuahua, México. ISSN: 2007-0411), Vol. 22, Núm. 3, pp. 14-33, Septiembre-Diciembre 2025. DOI: https://doi.org/10.20983/culcyt.2025.3.2.2. URI: https://erevistas.uacj.mx/ojs/index.php/culcyt/issue/view/887,https://erevistas.uacj.mx/ojs/index.php/culcyt/article/view/6916, (https://erevistas.uacj.mx/ojs/index.php/culcyt/article/view/6916/8918, 08/01/2026, 31/12/2025).
47. Mohammed, W.A.Y., Fattah, S., Saeed, K.M.O., Ibrahim, A.O., and Eltahier, S. 2025. "Enhancing the RC4 Algorithm by Eliminating the Initiative Vector (IV) Transmission", Engineering, Technology & Applied Science Research (e-ISSN: 1792-8036), 15(1), february, 20242–20248. DOI: https://doi.org/10.48084/etasr.9208. Available at: (ttps://etasr.com/index.php/ETASR/article/view/9208, 01/06/2025).
48. Rambe, B.M., Nababan, E.B., and Nasution, M.K. 2024. "Performance Analysis Of The Combination Of Blum Blum Shub And RC5 Algorithm In Message Security", JITE (Journal of Informatics and Telecommunication. Engineering, e-ISSN: 2549-6255), 7(2), january issue, 409-423. DOI: 10.31289/jite.v7i2.10937. Available at: (https://ojs.uma.ac.id/index.php/jite/article/view/10937, 06/01/2025).
49. Dang, Q.H., and Le, H.Q. 2022. "Improved cryptanalysis of the RSA algorithm using side-channel attacks", Journal of Information Security and Applications, vol. 65, no. 103313.

50. Luciano, D., and Prichett, G. 1987. "Cryptology: From Caesar Ciphers To Public-key Cryptosystems". The College Mathematics Journal, vol. 18, pp. 2-17. (http://www.jstor.org/stable/2686311, 06/06/2025).
51. Baker, M., and Schiller, J. 2015. "ECIES: Elliptic Curve Integrated Encryption Scheme", In Cryptography and Network Security, Springer, pp. 245-263. (https://medium.com/asecuritysite-when-bob-met-alice/elliptic-curve-integrated-encryption-scheme-ecies-encrypting-using-elliptic-curves-dc8d0b87eaa, 23/03/2025).
52. Hankerson, D., Hernandez, J.L., and Menezes, A.J. 2004. "Software implementation of elliptic curve cryptography over binary fields", Springer-Verlag Berlin Heidelberg 2000, [K. Ko¸c and C. Paar (Eds.) – CHES 2000, LNCS 1965], pp. 1–24. (https://idp.springer.com/authorize?response_type=cookie&client_id=springerlink&redirect_uri=https%3A%2F%2Flink.springer.com%2Fcontent%2Fpdf%2F10.1007%2F3-540-44499-8_1.pdf, 23/03/2025).
53. Montgomery, P.L. 1987. "Speeding up the Pollard rho method", Mathematics of Computation, vol. 48, no. 177, pp. 453-456.
54. NIST. 2013. "Special Publication 800-56A Revision 2: Recommended methods for key establishment using public key cryptography", NIST Special Publication 800-56A. (https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-56ar2.pdf&ved=2ahUKEwio1eCz3KGMAxWgJ0QIHYc4BXQQFnoECBsQAQ&usg=AOvVaw367-qADImRilvhabe1UtQr), (https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://csrc.nist.gov/pubs/sp/800/56/a/r2/final&ved=2ahUKEwio1eCz3KGMAxWgJ0QIHYc4BXQQFnoECBwQAQ&usg=AOvVaw183JO5CLTxYuENINrMwqgL, 23/03/2025).
55. Iavich, M., Kuchukhidze, T., and Gagnidze, A. 2024. "Post-quantum Digital Signature Using Verkle Trees And Lattices", SPCSJ, Scientific and Practical Cyber Security Journal [SCSA, Scientific Cyber Security Association, Tbilisi, Georgia, ISSN: 2587-4667], vol. 8, no. 3, pp. 35-52. (https://journal.scsa.ge/issues-archive/, 23/03/2025).
56. Fuegner, P. 2024. "Are RSA and AES Both at Risk From the Quantum Threat?", QuSecure, Inc. (https://www.qusecure.com/are-rsa-and-aes-both-at-risk-from-the-quantum-threat/#:~:text=The%20emergence%20of%20quantum%20computers,efficiently%20factoring%20large%20prime%20numbers, 2025-02-08).
57. Sengupta, S., and Ghosh, S. 2023. "Quantum Computing Encryption Threats: Why RSA and AES Are at Risk", Journal of Cryptographic Research.
58. Thakur, J., and Kumar, N. 2011. "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis", International Journal of Emerging Technology and Advanced Engineering, pp. 6-12.
59. Rangel, E. 2002. "Vecinos Envolventes para Variantes de la Regla del Vecino más Cercano", [MSc.Thesis], Instituto Tecnológico de Toluca, Metepec, México.
60. Rangel, E. 2022. "La Regla De Los k Vecinos Más Cercanos (k-NN) Basada En Distancia De Manhattan (City-Block) Para Mejorar La Clasificación De Patrones", In Quinto (V) Congreso Nacional De Investigación En Ciencia E Innovación De Tecnologías Productivas. Tecnológico Nacional De México, campus: Instituto Tecnológico de Cd. Altamirano, Estado De Guerrero, México, noviembre. (http://erangel.coolpage.biz/pappers/ edgarrangel2022.pdf, 06/06/2025).
61. Clark, A. 1994. "Modern optimisation algorithms for cryptanalysis", In Proceedings of the 1994 Second Australian and New Zealand Conference on Intelligent Information Systems, November 29 - December 2, pp. 258-262.
62. Griindlingh, W., and Van-Vuuren, J.H. 2003. "Using Genetic Algorithms to Break a Simple Cryptographic Cipher", (submitted 2002), Retrieved March 31, unpublished. (http://dip.sun.ac.za/~vuuren/abstracts/abstr_genetic.htm).
63. Kuncheva, L.I., and Jain, L.C. 1999. "Nearest Neighbor Classifier: Simultaneous editing and feature selection", Pattern Recognition Letters, vol. 20, pp. 1149-1156.

64. Matthews, R.A.J. 1993. "The use of genetic algorithms in cryptanalysis", Cryptologia, vol. 17, no. 4, pp. 187-201.
65. Reddaiah, B. 2019. "A Study on Genetic Algorithms for Cryptography", International Journal of Computer Applications, [Department of Computer Applications, Yogi Vemana University Kadapa, A.P, India, ISSN: 0975-8887], vol. 177, no. 28, pp. 1-4, december. DOI: http://dx.doi.org/10.5120/ijca2019919509, (https://www.researchgate.net/publication/338012809_A_Study_on_Genetic_Algorithms_for_Cryptography, 23/03/2024).
66. Sebas, C. 2023. "¿Qué son los Algoritmos Genéticos en las Inteligencias Artificiales?", Manuales y Tutoriales de Informatica,. (https://aprendeinformaticas.com/ia/, 23/03/2024).
67. Skalak, D.B. 1994. "Prototype and Feature Selection by Sampling and Random Mutation Hill Climbing Algorithms", In ML94, Proceedings of the Eleventh International Conference on Machine Learning, [Morgan Kaufmann], pp. 293-301.
68. Bruzzone, L., and Serpico, S.B. 1997. "Classification of Imbalanced remote-sensing data by neural networks", Elsevier Science B.V. , [0167-8655, 97, PH S0167-8655 (97) 00109-8]. DOI: https://doi.org/10.1016/S0167-8655(97)00109-8. (https://www.sciencedirect.com/science/article/abs/pii/S0167865597001098, 01/06/2025).
69. Goodfellow,.I., Bengio, Y., and Courville, A. 2021. "Deep learning", MIT Press.
70. Murphy, K.P. 2022. "Probabilistic machine learning: An introduction", MIT Press.
71. Iyengar, S.S., Kannan, R., and Ganapathi, S. 2021. "Inteligencia artificial y criptografía: Tendencias y desafíos", IEEE Transactions on Emerging Topics in Computing, vol. 9, no. 2, pp. 833-844.
72. Singh, A.K., Kumar, P., and Singh, R. 2021. "Aplicación de la inteligencia artificial en la criptografía: Una revisión", Journal of Intelligent Information Systems, vol. 67, no. 2, pp. 257-275.
73. Reddaiah, B. 2016. "A Study on Pairing Functions for Cryptography", IJCA (0975-8887), vol. 149, no. 10, pp. 4-7, september.
74. Liu, X., and Wang, X. 2022. "Quantum cryptanalysis of lattice-based cryptographic protocols", Physical Review X, vol. 12, no. 2 (021004).
75. Barandela, R., Sánchez, J.S., García, V., and Rangel, E. 2003. "Strategies for Learning in Class Imbalance Problems", Pattern Recognition [Rapid and Brief Comunication, Pergamon, ISBN: PII: S0031-3203(02)00257-1.0031-3203/02/], vol. 36, no. 3, pp. 849-851. DOI: https://doi.org/10.1016/S0031-3203(02)00257-1, (01/06/2025).
76. Cover, T.M., and Hart, P.E. 1967. "Nearest Neighbor Pattern Classification", IEEE Transactions on Information Theory, [e-ISSN: 1557-9654], vol. IT-13, january, pp. 21-27. DOI: 10.1109/TIT.1967.1053964. (https://ieeexplore.ieee.org/abstract/document/ 1053964/, 23/03/2024).
77. Lewis, D., and Catlett, J. 1994. "Heterogeneous Uncertainty Sampling for Supervised Learning", Proceedings of the 11th International Conference on Machine Learning, ICML'94, [New Brunswick, New Jersey, Morgan Kaufmann], pp. 148-156.
78. Rangel, E., Rangel, C.M., and Rangel, K.U. 2025g. "Camuflaje de Textos Cifrados Utilizando Inteligencia Artificial para Mejorar la Seguridad del Algoritmo AES-256, Convirtiéndolo en un Esquema de Encriptado Dinámico", Revista Electrónica de Divulgación de la Investigación del SABES (Revista de la Universidad del SABES. Editada por Sistema Avanzado de Bachillerato y Educación Superior en el Estado de Guanajuato. México). ISSN: 2007-3542, vol. 30, pp. 39-75, edición diciembre 2025 - enero 2026. https://sabes.edu.mx/revista-electronica/29/#, (https://sabes.edu.mx/revista-electronica/29/docs/3_Camuflaje_de_textos_cifrados.pdf, 19/12/2025).
79. PyCryptodome. 2025. "Crypto.Cipher package. Introduction", Readthedocs.io, (https://pycryptodome. readthedocs.io/en/ latest/src/cipher/cipher.html, 30/03/2025).
80. PyPI. 2024. "Pycryptodome 3.21.0", Python Software Foundation. (https://pypi.org/project/ pycryptodome/, 13/12/2024).