A Note on Public Key Cryptosystems

Yashika Singh and Shreya Jaiswal
Pranveer Singh Institute of Technology, Kanpur

ABSTRACT

Public key or asymmetric cryptosystems use public-private key pair for the secure transmission of data. RSA and ECC (Elliptic Curve Cryptography/Cryptosystems) are widely used cryptosystems in this category. Public key cryptosystems rely on mathematical problems known as hard problems. The security of these cryptosystems is based on these hard problems. Public key cryptosystems solve the key transportation problem of symmetric key cryptosystems and able to provides digital signatures also.

Keywords: **RSA, ECC (Elliptic Curve Cryptography/Cryptosystems), Security, Symmetric Key, Public Key**

INTRODUCTION:

Public key or asymmetric key cryptosystems use – public-private key pair. The data is encrypted by receiver's public key and can be decrypted by receiver's private key. Since the private key is never transmitted anywhere during the entire communication, public key cryptosystems provide high level of security. Data communication is a necessity of life in modern world so the importance of public key cryptosystems increases very sharply not only in cryptography and its allied areas [1-9] but also in wireless communication scenarios [10-15] and network security applications [16-20]. In cryptography, all cryptosystems can be divided into two categories. First is symmetric key cryptosystems and second is public key cryptosystems. In symmetric key cryptosystems, both sender and receiver use the same secret key for securing the data. The following figures show the difference between the above mentioned cryptosystems.

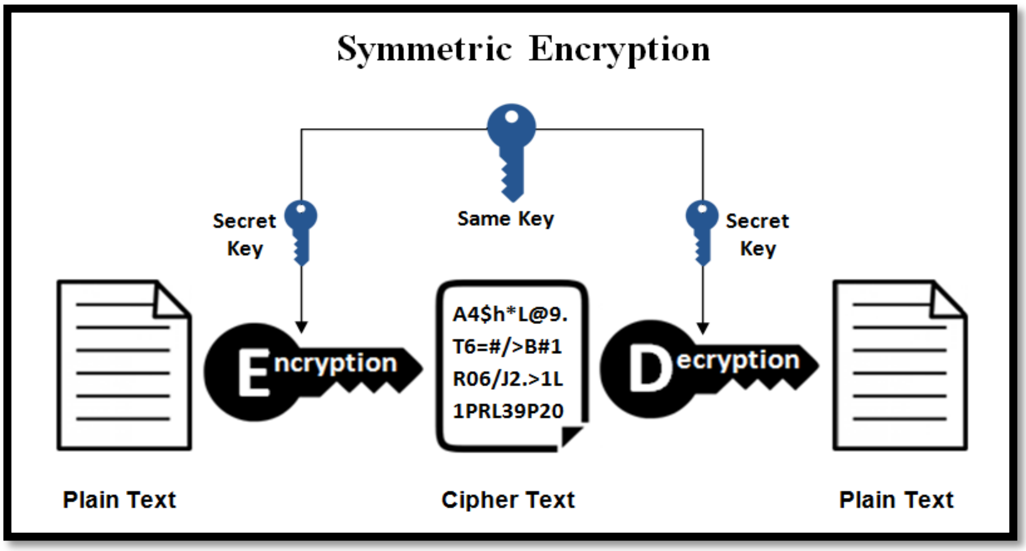


Fig.1. Showing Symmetric key encryption and decryption using the same key

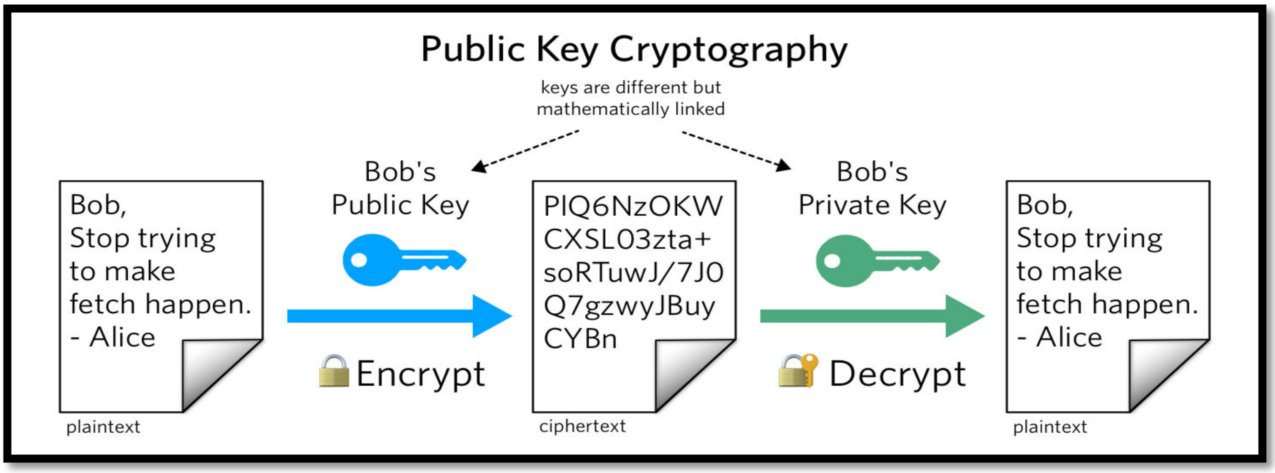
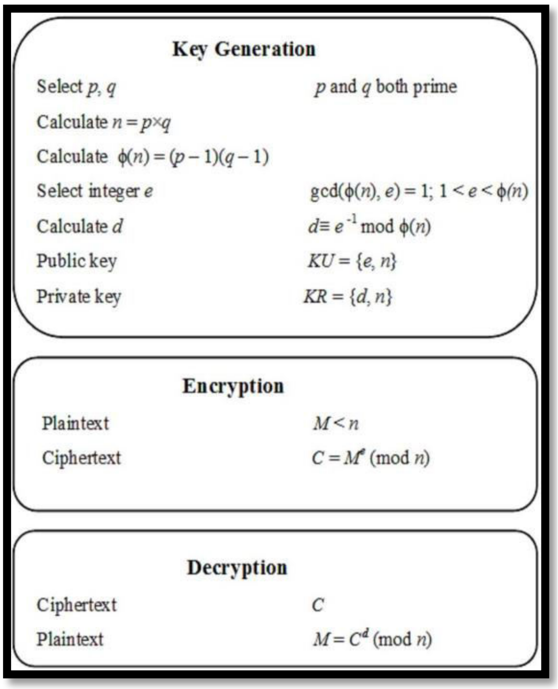

Public Key Cryptography
keys are different but mathematically linked
Bob's Public Key
Bob's Private Key
Bob, Stop trying to make fetch happen. - Alice
plaintext
Encrypt
PIQ6NzOKW CXSL03zta+ soRTuwJ/7J0 Q7gzwyJBuy CYBn
ciphertext
Decrypt
Bob, Stop trying to make fetch happen. - Alice
plaintext

Fig.2. Showing public key encryption and decryption using the key pair

Now we discuss some of the famous public key cryptosystems [21-22].

- **RSA**: RSA is the most trusted asymmetric key cryptosystem. It is based on prime factorization problem. One needs to select two prime numbers p and q so that n=pq. It is important to mention that p and q should be large enough for security. The full RSA method is described in the below figure for better understanding.



Key Generation

Select p, q	p and q both prime
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} \bmod \phi(n)$
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

Encryption

Plaintext	$M < n$
Ciphertext	$C = M^e \pmod{n}$

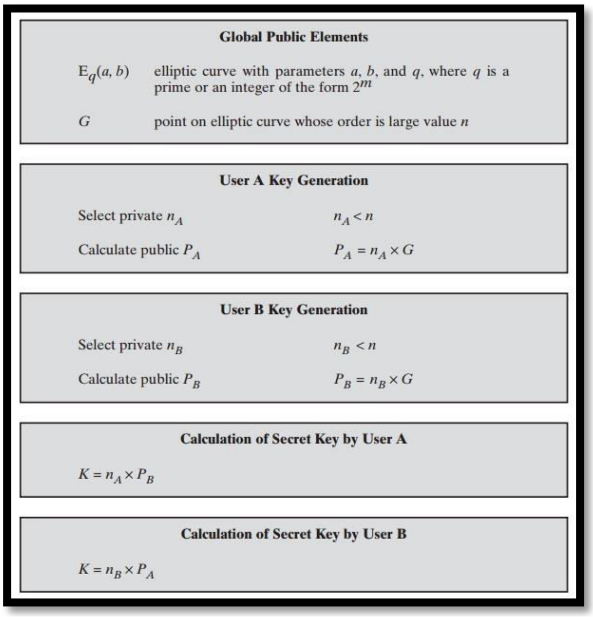
Decryption

Ciphertext	C
Plaintext	$M = C^d \pmod{n}$

Fig. 3. Showing the complete RSA procedure

- **Advantages:**
  - Easily implementable on various platforms
  - Highly secure as it is based on prime factorization
  - Widely accepted and trusted
- **Disadvantages:**
- Security is dependent on selection of prime numbers
- High computational overheads
- Public keys must be authenticated by a third party

- **ECC**: ECC provides equivalent level of encryption as provided by RSA with a shorter key length so naturally the speed of ECC is also faster than RSA. RSA-1024 bits key length security can be achieved by 160-223 bits key security of ECC. The basics of key generation in ECC are defined in the figure below.



Global Public Elements

$E_q(a, b)$	elliptic curve with parameters a, b, and q, where q is a prime or an integer of the form 2^m
G	point on elliptic curve whose order is large value n

User A Key Generation

Select private n_A	$n_A < n$
Calculate public P_A	$P_A = n_A \times G$

User B Key Generation

Select private n_B	$n_B < n$
Calculate public P_B	$P_B = n_B \times G$

Calculation of Secret Key by User A

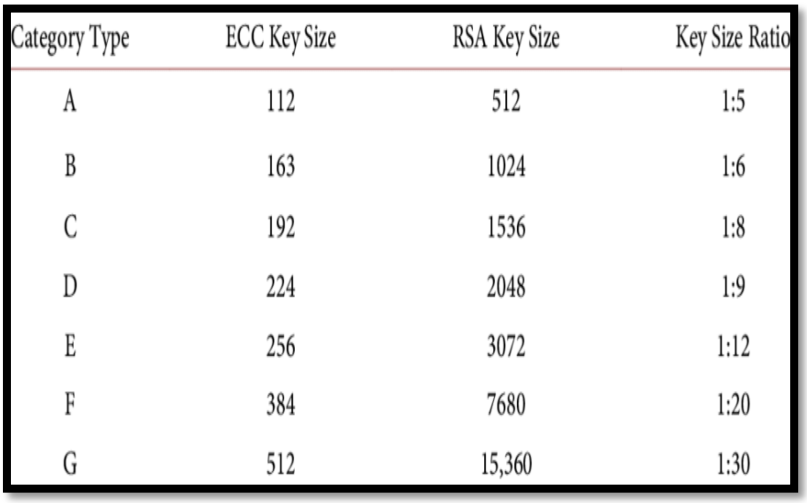
$K = n_A \times P_B$

Calculation of Secret Key by User B

$K = n_B \times P_A$

Fig.4. Showing the key generation in ECC

The key size comparison of ECC and RSA is given in the below figure.



Category Type	ECC Key Size	RSA Key Size	Key Size Ratio
A	112	512	1:5
B	163	1024	1:6
C	192	1536	1:8
D	224	2048	1:9
E	256	3072	1:12
F	384	7680	1:20
G	512	15,360	1:30

Fig.5. Showing the key size comparison between RSA and ECC

- **Advantages**:
  - ➢ Shorter key size
  - ➢ High level of security
  - ➢ Easily implementable
- **Disadvantages**:
  - ➢ Size of encrypted message is increased
  - ➢ Complex algorithm
  - ➢ Not widely accepted as RSA

CONCLUSION:

It can be concluded that public key cryptosystems use public-private key pair and solve the key transportation problem of symmetric key cryptosystems. The message is encrypted using the public key and private key is always kept secret by the participating entities. RSA and ECC are two main public key cryptosystems. RSA is the most trusted and widely accepted public key cryptosystem till date but uses large key for high level of security. On the other side, ECC provides equivalent level of security with reduced key size but not as trusted and widely accepted as RSA.

REFERENCES

[1]. V. Shukla, A. Chaturvedi, N. Srivastava, Nanotechnology and cryptographic protocols: issues and possible solutions, Nanomaterials and energy, volume 8, issue 1, 2019, 1-6,
DOI: 10.1680/jnaen.18.00006

[2]. M.K. Misra, A. Chaturvedi, S.P. Tripathi, V. Shukla, A unique key sharing protocol among three users using non-commutative group for electronic health record system, Journal of discrete mathematical sciences and cryptography, volume 22, issue 8, 2019, 1435–1451,
DOI: 10.1080/09720529.2019.1692450

[3]. A. Chaturvedi, N. Srivastava, V. Shukla, A secure wireless communication protocol using Diffie-Hellman key exchange, International journal of computer applications, volume 126, number 5, 2015, 35-38,
DOI: 10.5120/ijca2015906060

[4]. V. Shukla, A. Chaturvedi, M.K. Misra, On authentication schemes using polynomials over non commutative rings, Wireless personal communications, volume 118, issue 1, 2021, 1-9,
DOI: https://doi.org/10.1007/s11277-020-08008-4

[5]. V. Shukla, A. Mishra, S. Agarwal, A new one time password generation method for financial transactions with randomness analysis, Innovations in electrical and electronic engineering (Part of the lecture notes in electrical engineering book series (LNEE, volume 661)), 2020, 713-720,
DOI: https://doi.org/10.1007/978-981-15-4692-1_54

[6]. V. Shukla, A. Mishra, A. Yadav, An authenticated and secure electronic health record system, IEEE international conference on information and communication technology, 2019, 1-5,
DOI: 10.1109/CICT48419.2019.9066168

[7]. A. Chaturvedi, V. Shukla, M.K. Misra, Three party key sharing protocol using polynomial rings, 5th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), 2018, 1-5,
DOI: 10.1109/UPCON.2018.8596905

[8]. V. Shukla, A. Chaturvedi, N. Srivastava, Secure wireless communication protocol: to avoid vulnerabilities in shared authentication, Communications on applied electronics, volume 7, number 6, 2017, 4-7,
DOI: 10.5120/cae2017652680

[9]. V. Shukla, M.K. Misra, A. Chaturvedi, Journey of cryptocurrency in India in view of financial budget 2022-23, Cornell university arxiv, 2022, 1-6,
DOI: https://doi.org/10.48550/arXiv.2203.12606

[10]. V. Shukla, N. Srivastava, A. Chaturvedi, A bit commitment signcryption protocol for wireless transport layer security (wtls), IEEE international conference on electrical, computer and electronics engineering , 2016, 83-86,
DOI: 10.1109/UPCON.2016.7894629

[11]. V. Shukla, A. Chaturvedi, N. Srivastava, A new secure authenticated key agreement scheme for wireless (mobile) communication in an EHR system using cryptography, Communications on applied electronics, volume 3, number 3, 2015, 16-21,
DOI: 10.5120/cae2015651903

[12]. A. Chaturvedi, N. Srivastava, V. Shukla, S.P. Tripathi, M.K. Misra, A secure zero knowledge authentication protocol for wireless (mobile) ad-hoc networks, International journal of computer applications, volume 128, number 2, 2015, 36-39,
DOI: 10.5120/ijca2015906437

[13]. V. Shukla, A. Chaturvedi, N. Srivastava, Authentication aspects of dynamic routing protocols: associated problem & proposed solution, International journal of recent technology and engineering, volume 8, issue 2, 2019, 412-419,
DOI: 10.35940/ijrte.B1503.078219

[14]. V. Shukla, A. Kushwaha, S.S. Parihar, S. Srivastava, V. P. Singh, Authenticated wireless information display system using GSM module, Communications on applied electronics, volume 5, number 3, 2016, 7-11,
DOI: 10.5120/cae2016652251

[15]. V. Shukla, A. Chaturvedi, N. Srivastava, Double layer cryptographic protocol for mobile ad-hoc networks (MANETs) by commitment scheme, Communications on applied electronics, volume 7, number 9, 2017, 32-36,
DOI: 10.5120/cae2017652716

[16]. V. Shukla, A. Chaturvedi, N. Srivastava, A secure stop and wait communication protocol for disturbed

networks, Wireless personal communications, volume 110, 861-872, 2019,
DOI: https://doi.org/10.1007/s11277-019-06760-w

[17]. V. Shukla, A. Mishra, A new sequential coding method for secure data communication, IEEE international conference on computing, power and communication technologies, 2020, 529-533,
DOI: 10.1109/GUCON48875.2020.9231252

[18]. A. Chaturvedi, V. Shukla, M.K. Misra, A random encoding method for secure data communication: an extension of sequential coding, Journal of discrete mathematical sciences and cryptography, volume 24, issue 5, 2021, 1189-1204,
DOI: https://doi.org/10.1080/09720529.2021.1932902

[19]. V. Shukla, A. Chaturvedi, N. Srivastava, A new one time password mechanism for client-server applications, Journal of discrete mathematical sciences and cryptography, volume 22, 2019, 1393-1406,
DOI: 10.1080/09720529.2019.1692447

[20]. V. Shukla, M.K. Misra, A. Chaturvedi, A new authentication procedure for client-server applications using HMAC, Journal of discrete mathematical sciences and cryptography, volume 24, issue 5, 2021, 1241-1256,
DOI: https://doi.org/10.1080/09720529.2021.1932908

[21]. A.J.Menezes, P.C.V.Oorschot, S.A.Vanstone, Handbook of applied cryptography, fifth edition, CRC press Inc., USA, ISBN: 9780849385230, 2001.

[22]. W.Stallings, Cryptography and network security, principles and practices, seventh edition, Prentice Hall, ISBN-13:978-0134444284, ISBN-10:0134444280, 2005.