Hybrid Cryptography for connected wireless devices

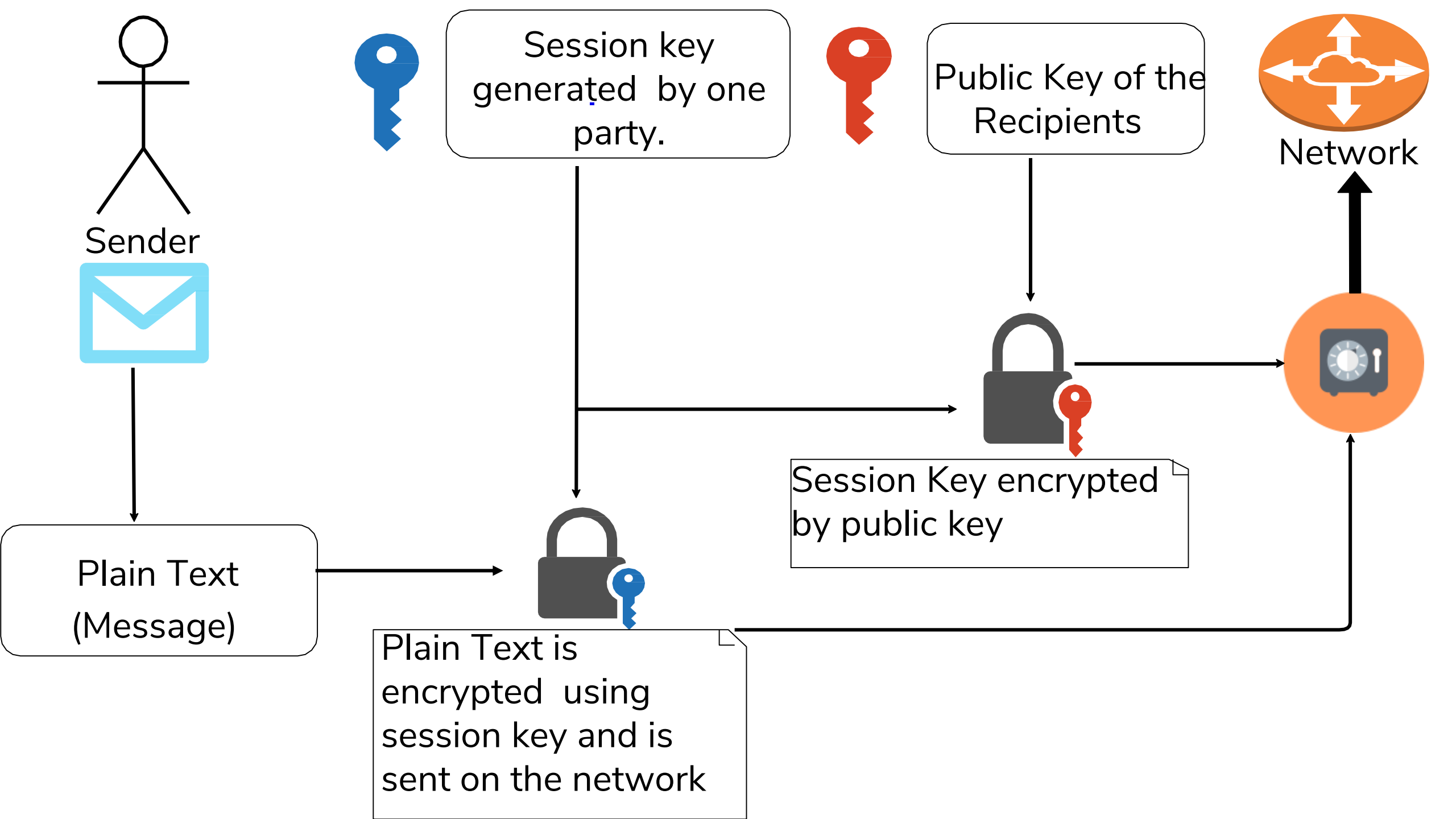
1. Introduction
2. Related Works
3. Research Methodology
4. Results
5. Conclusion
6. References

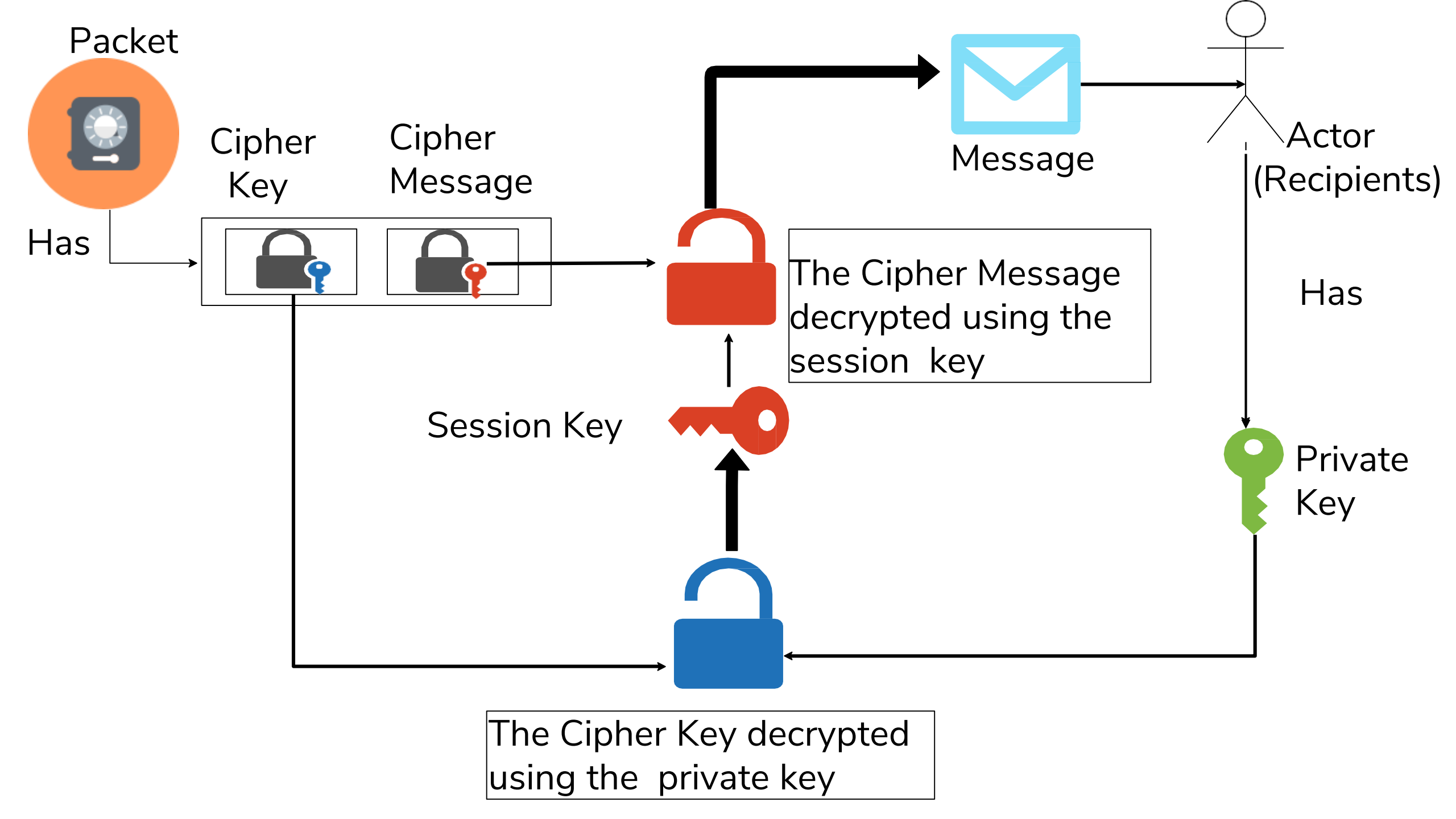
"With the growth in IOT,Cloud computing, etc. security is at a risk. The Greatest security control you can deploy is cryptography."

A project by Vaidehi Manoj Ghime.
Department Of Computer Science And Engineering,
Indian Institute Of Information Technology,Nagpur.

Introduction:

- ➔ Limited energy, computational and memory resources.
- ➔ Cryptography Algorithms require high computational power.
- ➔ Hybrid Cryptography combines:
  - ◆ convenience of public key cryptosystem.
  - ◆ efficiency of the symmetric key cryptosystem.
- ➔ main aim is to provide an efficient algorithm for Secure Data Communication using minimum memory and power.

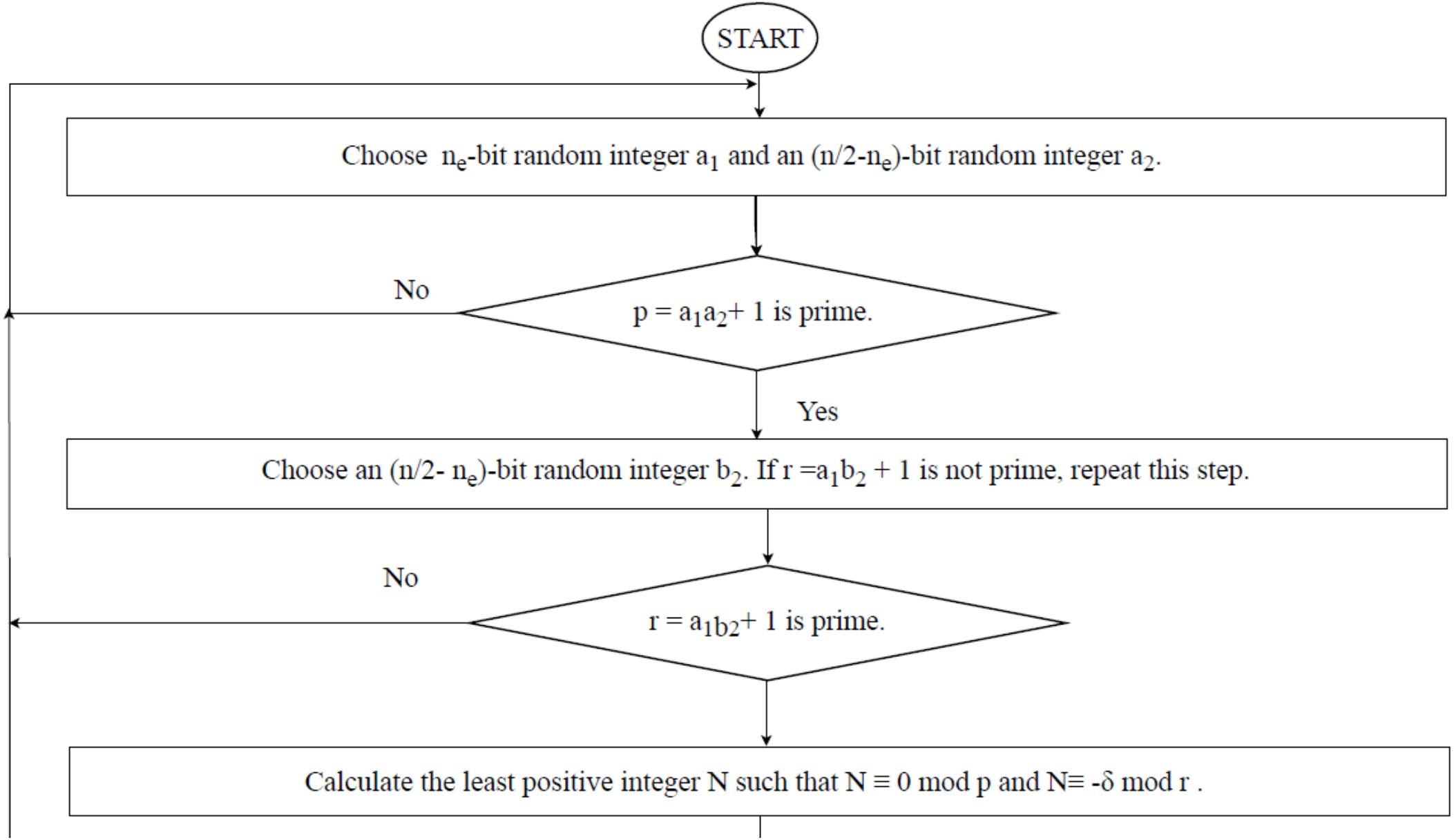

Session key generated by one party.
Public Key of the Recipients
Network
Sender
Session Key encrypted by public key
Plain Text (Message)
Plain Text is encrypted using session key and is sent on the network

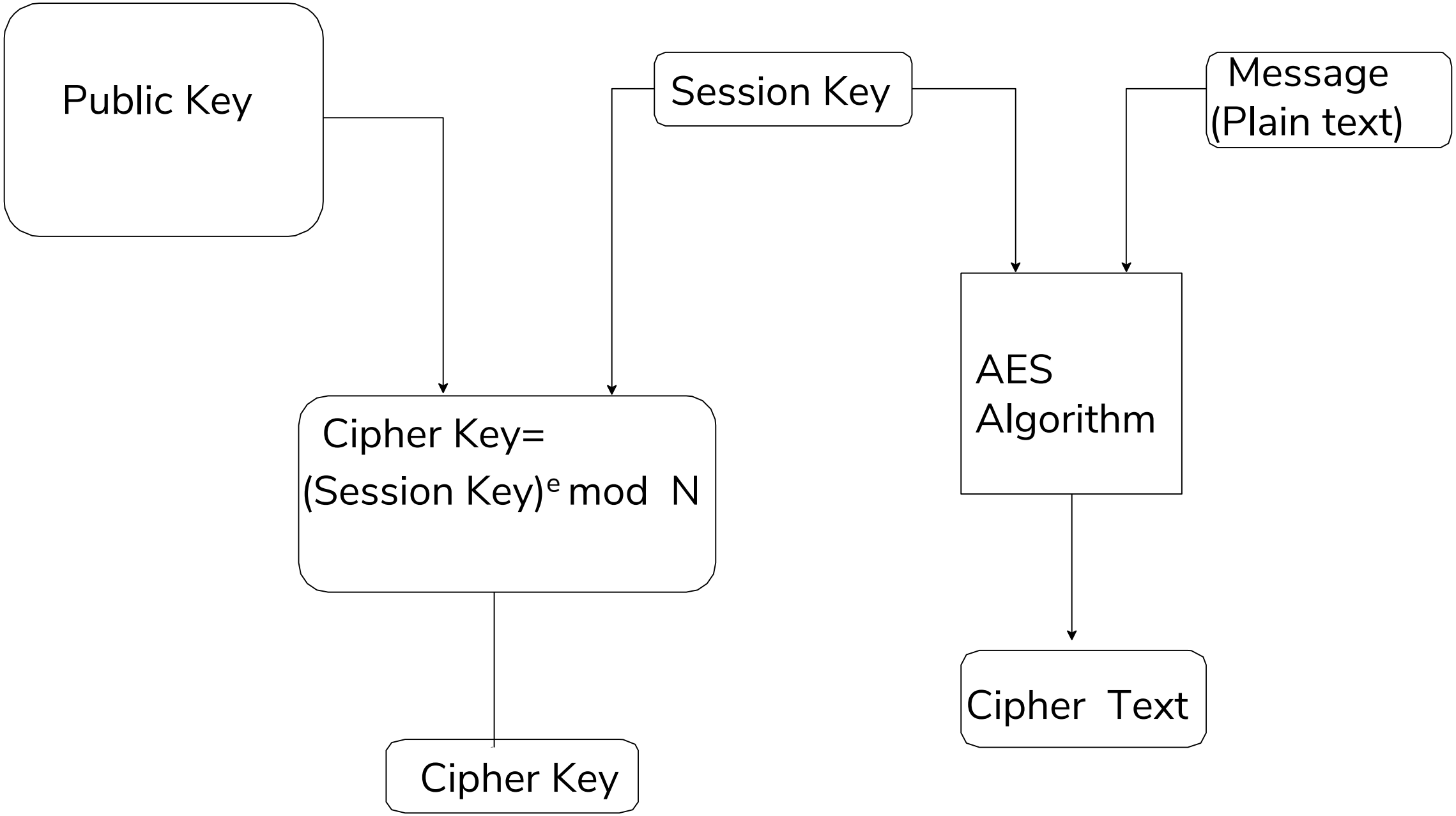

Packet
Has
Cipher Key
Cipher Message
Message
Actor (Recipients)
Has
The Cipher Message decrypted using the session key
Session Key
Private Key
The Cipher Key decrypted using the private key

Related Works:

Author (Year)	Proposed Approach
Prakash, S., & Rajput[1] (2018)	An Efficient Algorithm exploiting the advantages of AES - symmetric key algorithm and ECC- asymmetric key algorithm consuming less resources and time.
Verma, S., & Garg, D.[2] (2014)	reduce the memory requirement of RSA cryptosystem so as to use RSA in memory constrained environment.
Mahalle, V. S., & Shahade, A. K.[5] (2014)	proposed a hybrid encryption algorithm using RSA and AES algorithms for providing data security to the user in the Cloud. The biggest advantage it provides us is that the keys are generated on the basis of system time and so no intruder can even guess them there by giving us increased security along with convenience

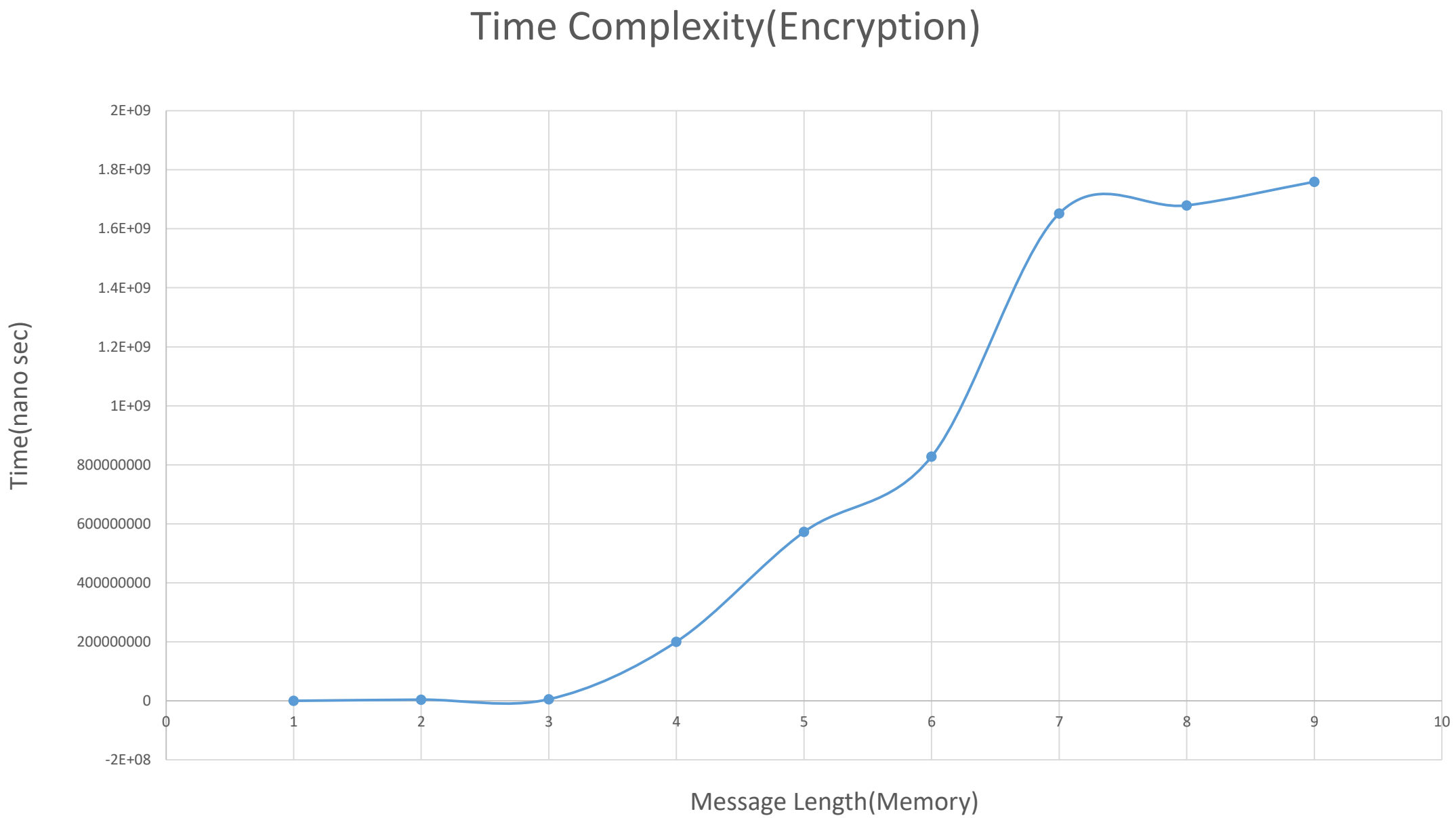
Research Methodology:

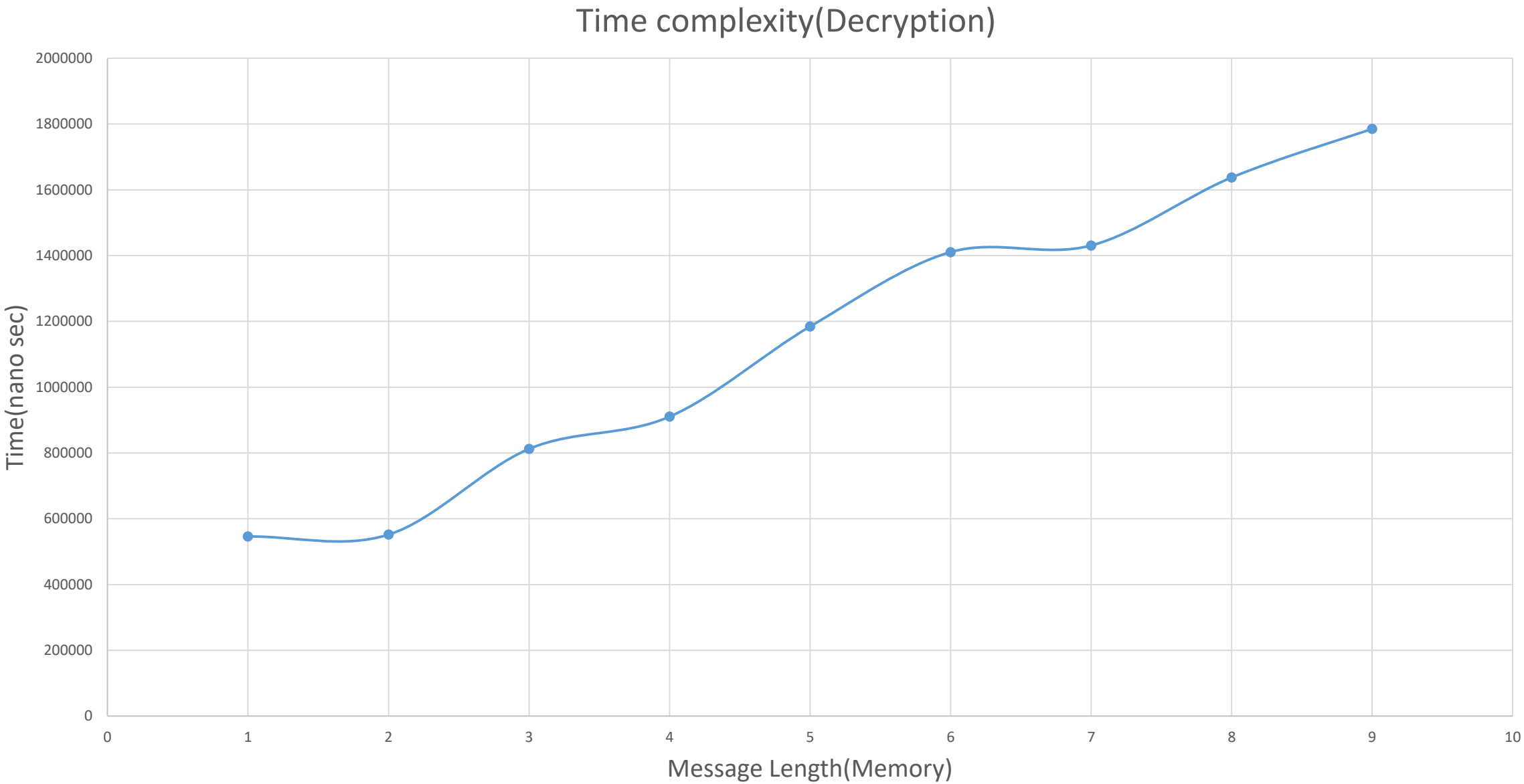



Public Key
Session Key
Message
(Plain text)
Cipher Key=
(Session Key)^e mod N
AES
Algorithm
Cipher Key
Cipher Text

Results:

- As the user/devices increases the no of keys increases linearly and not exponentially.
- One of the most secure Cryptographic algorithm cannot be broken by today’s Supercomputers too.
- Data Confidentiality, Integrity.
- Encryption and decryption is not complex due to use of AES and does not consumes time.
- Succeeded to bring an memory and time efficient cryptographic algorithm .


Time Complexity(Encryption)
Time(nano sec)
2E+09
1.8E+09
1.6E+09
1.4E+09
1.2E+09
1E+09
800000000
600000000
400000000
200000000
0
-2E+08
0
1
2
3
4
5
6
7
8
9
10
Message Length(Memory)


Time complexity(Decryption)
Time(nano sec)
2000000
1800000
1600000
1400000
1200000
1000000
800000
600000
400000
200000
0
0
1
2
3
4
5
6
7
8
9
10
Message Length(Memory)

Conclusion:

- ➔ scope of wireless devices ,cloud based services is increasing.
- ➔ need to provide secure data communication with the use of limited resources.
- ➔ used the advantages of RSA algorithm for key generation and sharing and AES algorithm for encryption and decryption.
- ➔ RSA algorithm is modified to the memory efficient version.

References:

1. Prakash, S., & Rajput, A. (2018). Hybrid Cryptography for Secure Data Communication in Wireless Sensor Networks. *Springer Nature Singapore Pte Ltd. 2018*,589-599. Retrieved April 9, 2018.
2. Verma, S., & Garg, D. (2014). RSA Variant with Efficient Memory Usage. *International Conference on Advances in Engineering and Technology (ICAET2014) March 29-30, 2014 Singapore*,209-211. doi:10.15242/iie.e0314095.
3. Thirumalai, C., & Kar, H. (2017). Memory efficient multi key (MEMK) generation scheme for secure transportation of sensitive data over cloud and IoT devices. *2017 Innovations in Power and Advanced Computing Technologies (i-PACT)*. doi:10.1109/ipact.2017.8244948.
4. Najar, J. M., & Dar, S. B. (2014). A New Design Of A Hybrid Encryption Algorithm. *International Journal Of Engineering And Computer Science,3*, 9169-9171. doi:11 November
5. Mahalle, V. S., & Shahade, A. K. (2014). Enhancing the data security in Cloud by implementing hybrid (Rsa & Aes) encryption algorithm. *2014 International Conference on Power, Automation and Communication (INPAC)*. doi:10.1109/inpac.2014.6981152