# Securing Robotic Communication using Multiple Security Techniques

Sadeq Othman Al-Hamouz
The World Islamic Sciences and Education University,
Amman, 11947, Jordan

## ABSTRACT
It is undeniable that security is becoming a major concern in almost every aspect of digital applications, like remotely controlling a robot, where any interference with the sent command, or received data is not accepted and could have negative impact on the robot's mission.

In this research, robotic commands were secured using different techniques that vary between securing the transmission channels, and securing the data transmitted itself, while securing the encryption keys for the encrypted data. The transmission used Received Signal Strength Indicator (RSSI) modules signal for Radio Frequency (RF) modules (in the test case XBEE and NRF24L01+ modules were used) and ping time for internet modules (SIM808 and CC3000), choosing the strongest signal of each module and send data through them. While the data was encrypted using three encryption algorithms: RSA, AES and TwoFish. The test results from attempts to hack this system showed that it requires too much time (compared with using only one encryption technique) using a computer with high processing capacities and previous knowledge of the used security techniques.

## General Terms
Message Encryption, Robot communication, communication interface.

## Keywords
Robot, Encryption, RSA, AES, TwoFish, RSSI, RF.

## 1. INTRODUCTION
A remotely controlled robot is becoming used more often in a variety of applications, both in civil and military fields. The controller can be located several meters (or kilometers) away from the robot, so the communication signal need to have proper broadcasting range, in addition to having techniques that prevents (or minimizes) any interference with the signal, like jamming or hacking.

The main idea in this research is to prevent hacking the Robot's communications by using secure encryption (used three algorithms over multiple stages: RSA, AES and twofish), the developed algorithm aims at preventing spoofing the signal by using each encryption key one time only before deleting it from the robot's (and controller's station) memory. The algorithm helps in preventing missing Robot communication signal or interference by using multiple wireless interfaces that also confuses an attacker as they will not be able to monitor all interfaces and get full data transfer stream between base station and Robot.

RSA was named after its creators (Rivest-Shamir-Adleman) and it is considered the most used encryption technique [1]. It is an asymmetric ciphering technique that uses large integers (mostly 1024bits) and ciphers data over only one round. Figure 1 shows the basic RSA encryption/decryption technique.

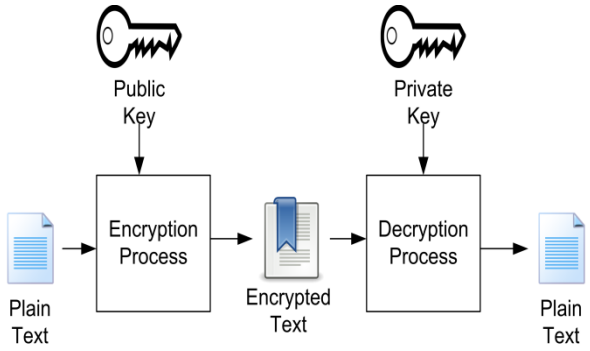


**Figure 1: RSA algorithm [1]**

AES (Advanced Encryption standard) is developed by Vincent Rijmen, Joan Daeman in 2001 [2] and financed by the United States Government as an encryption technique for classified data. This technique applies encryption over three blocks [10], each of 128bit size. Figure 2 shows the basic flowchart of AES encryption algorithm.

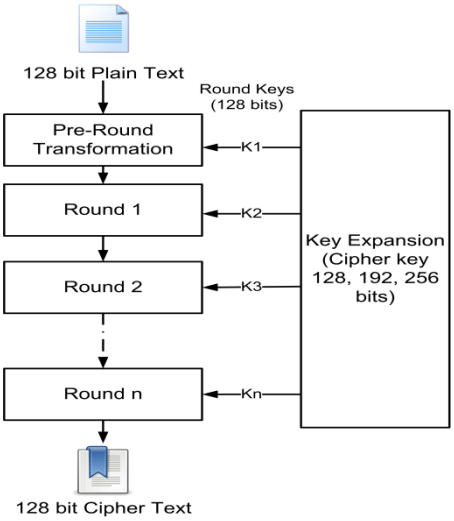


**Figure 2: Flowchart of how AES algorithm [1]**

Twofish cipher was created by Bruce Schneier in 1998 [3]. With the innovation and widespread of smart cards, the need for an encryption technique that can run on small processors was most needed. This algorithm encrypts data over three cipher blocks each of 128bits, and goes over 16 rounds, though these numbers are customizable since this algorithm is open for modification. Figure 3 shows one round of the basic twofish encryption algorithm.

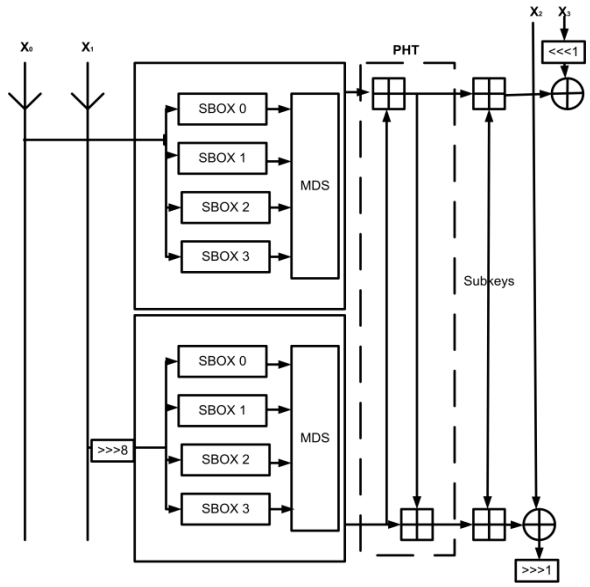


**Figure 3: TowFish basic algorithm [5]**

In this research, the main station uses the above mentioned algorithms to encrypt Robot data: RSA, Twofish and AES. RSA algorithm works by generating two keys for data, a public key that is sent to the message receiver and a private key that already exists (pre-loaded) with receiver and used to decode the message. Twofish and AES algorithms work in different ways; they can encrypt data by entering a password used for encryption/decryption process.

Authentication using RSA was proven to be not very efficient with remote controllers [4], so some researchers update and made modifications to the original scheme of RSA encryption scheme to be more effective against attacks, like [5] and [6] and many others.

Remote authentication can be used in many applications along with robot communication security, like e-banking, online pay-tv and others according to [7] who used RSA encryption in remote authentication combined with one-way hash function and smart card. Some used remote commands encryption with smart home appliances control [8]

Securing robot-to-robot or robot-control station communications was studied by many researchers, like [9] and [11]. The authors of [9] for example, proposed a two-fold technique for securing exchanged messages; RSA technique for digital signature and distributing authentication keys, and AES for encrypting the message itself, with a sixteen bit, eight degree primitive polynomials. To decrease the computational overhead, they proposed using an ElGamal scheme with public/private key elliptic curve encoding after the first two robot message transaction.

## 2. THE ALGORITHM

Before sending the robot in its mission, it is loaded (by physical connection) with decryption data table that includes both private and public keys that will be used during remote communications. The main station starts by receiving needed command from the controller, then encrypting it using RSA algorithm, save the public key for later use, then take the encrypted message and encrypt it again using Twofish, save password on side and then combine both public key and password together to a single message and encrypt it using AES algorithm. Now there's dual encrypted message and encrypted public keys and a single password (that the Robot already knows and there's no need to send it).

The communication starts from main station where it starts by testing all Received Signal Strength Indicator (RSSI) modules signal for Radio Frequency (RF) modules (in the test case XBEE and NRF24L01+ modules were used) and ping time for internet modules (SIM808 and CC3000), and then determine strongest 2 signals to send information through them (using one internet module and one RF module). Figure 4 shows the sequence of actions at the base station (the controller's side).

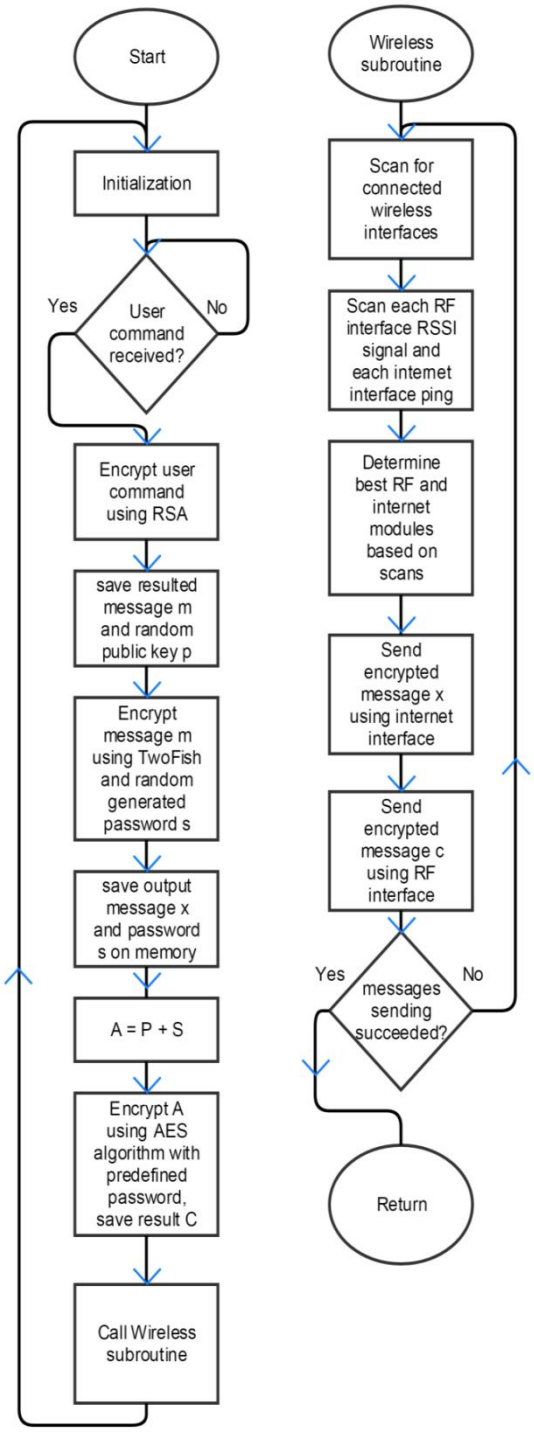


**Figure 4: Controller's side program flowchart**

The encrypted message will be sent to selected internet module, and encrypted keys will be sent to selected RF module at same time. The Robot now has all the information and will start decrypting the message it received through RF module (AES encrypted message) by using predefined password, then it will extract password and public key, use the password to decrypt the message received through the internet module (Twofish encrypted) and then use public key to decrypt resulted message from decrypting original message (RSA encrypted), then it will extract the command and perform it. Figure 5 shows the flowchart of receiving and decrypting messages at the robot's side.

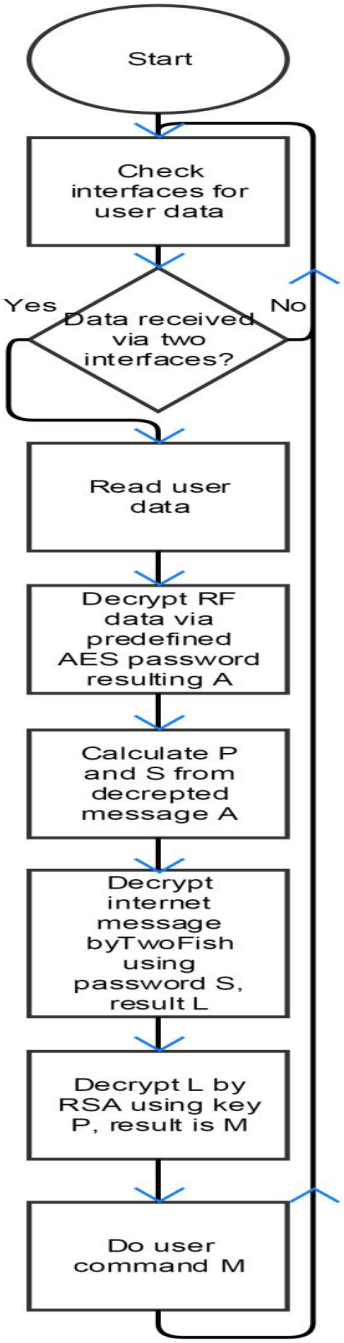


**Figure 5: Robot program flowchart**

## 3. ADVANTAGES OF THE PROPOSED ALGORITHM

The proposed method excels over other methods in many ways, in terms of security of exchanged messages, along with speed of communications (given the number of operations that are required to get maximum security). These benefits are summarized as follows:

- Dividing data to multiple interfaces assures higher efficiency as it reduces traffic of data sent, assures that an attacker will not have all needed information to attack the line as they will not likely have access to all wireless interfaces, besides, if they flood a line the Robot will have backup interfaces and thus communication will not be lost.
- Using multiple encryption algorithms will make the attacker struggle in decrypting them, and even if a message is decrypted correctly the result will be a message that the attacker does not understand (encrypted one also) and thus the attacker will think that the key used is incorrect and will not be able to divide between a correctly decrypted message and a wrongly decrypted one.

## 4. PERFORMANCE MEASUREMENT

To test the proposed system a simple message containing the word "H" was transmitted. the word was encrypted and sent to Robot with a different algorithms, while there were a computer in the middle running Linux Kali and connected with wireless receiver interfaces (same as Robot interfaces) trying to crack the sent message via brute force attack. Table 1 shows the results of comparison.

**Table 1: Comparing time needed to crack robot command encrypted with proposed technique with other encryption methods**

| Attacked algorithm (128 bit) | Cracking time (second) | Increased difficulty % (RSA as reference) |
|---|---|---|
| RSA | 4980 | 0% (reference point) |
| TwoFish | 5104 | 2.5% |
| AES | 3500 | -29.7% |
| Proposed Algorithm | 118640 | 2282.3% |

For RSA and AES, a readymade python scripts where used to brute force result, while for TwoFish and proposed algorithm, a special script where written from scratch to brute force results, assuming that the cracker already knows how the proposed algorithm works exactly, otherwise, it will take the attacker too much time to guess the combination of algorithm used by the algorithm.

By increasing proposed algorithm encryption to 1024 bit, computer program ran about 40 hours and provided out of memory error (128 GB RAM) before it was even close to crack first (and only letter in this case) the letter "H". Figure 6 shows the time needed to crack the message "H" sent to the robot compared to using one encryption technique to encrypt the same message.

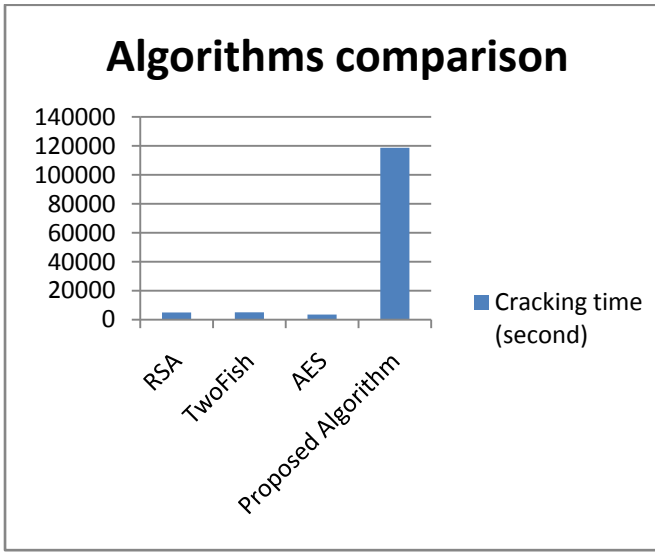


**Figure 6: Comparing using the integrated encryption technique with single encryption to crack a small message**

## 5. CONCLUSION

The proposed system provided better security measurements for robotic commands exchange. This security is most needed for robots that work in sensitive fields in which any alteration to the received (or sent) cannot be tolerated since it would have huge negative effects. The use of combined encryption techniques over the stages of communication proved to be way secured than using only one technique, though it would take longer time to process, but since robotic commands are very small in size of message to encrypt (mostly 2 or three characters) then this obstacle is trivial and can be overlooked. Other security techniques could be implemented and compared to the scheme proposed in this research work in the future to prove that this technique is most suitable for robotic communications' security.

## 6. REFERENCES

[1]. Bhanot, R., & Hans, R. (2015). A review and comparative analysis of various encryption algorithms. International Journal of Security and Its Applications, 9(4), 289-306.

[2]. Daemen, J., & Rijmen, V. (2013). The design of Rijndael: AES-the advanced encryption standard. Springer Science & Business Media.

[3]. Schneier, B., Kelsey, J., Whiting, D., Wagner, D., Hall, C., & Ferguson, N. (1998). Twofish: A 128-bit block cipher. NIST AES Proposal, 15.

[4]. Chang, C. C., & Hwang, K. F., (2003). Some Forgery Attacks on a Remote User Authentication Scheme Using Smart Cards. Informatics, Lith. Acad. Sci., 14(3), pp. 289-294.

[5]. Shen, J. J., Lin, C. W., & Hwang, M. S., (2003) Security enhancement for the timestamp-based password authentication scheme using smart cards. Computers & Security, 22(7), pp. 591-595.

[6]. Giri, D., Maitra, T., Amin, R., & Srivastava, P. D (2015), An efficient and robust RSA-based remote user authentication for telecare medical information systems. Journal of medical systems, 39(1), pp.1-9.

[7]. Chandrakar, P., & Om, H. (2015). RSA based two-factor remote user authentication scheme with user anonymity. Procedia Computer Science, 70, 318-324.

[8]. Jasim, M. M. (2014). A Secure Home Appliances Remote Control Model (Doctoral dissertation, Middle East University).

[9]. Yfantis, E. A., & Fayed, A. (2014). Authentication and secure robot communication. International Journal of Advanced Robotic Systems, 11(2), 10.

[10]. Islam, M. N., Mia, M. M. H., Chowdhury, M. F., & Matin, M. A. (2008, August). Effect of security increment to symmetric data encryption through AES methodology. In Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2008. SNPD'08. Ninth ACIS International Conference on (pp. 291-294). IEEE.

[11]. Singh, L., & Bharti, R. K. (2013). Comparative performance analysis of cryptographic algorithms. International Journal of Advanced Research in Computer Science and Software Engineering, 3(11), 43-52.