© Journal of the Technical University - Sofia
Plovdiv branch, Bulgaria
"Fundamental Sciences and Applications"
Vol. 25, 2019

Designing a Communication System for Secure Access to Network Devices

Tarık Yerlikaya and Senol Sen

Trakya University Ahmet Karadeniz Campus Department of Computer Engineering Edirne/Turkey

tarikyer@trakya.edu.tr, senolsen@trakya.edu.tr

Abstract. Start Network devices are generally programmed over the serial ports (COM-RS232) or over the network via telnet protocol or ssh protocol. The communication process via the Telnet protocol and COM port is done unencrypted. Therefore, there is a possibility to listen and change the communication by an intervening hacker. In order to prevent this, the hardware is designed described below. With this developed system, serial communication has been encrypted by adding RSA encryption using hardware between network devices which needs configuration with PC.

1. Introduction

Nowadays, the use of information technologies is spreading and increasing rapidly. Information, computer and information systems security are at the forefront of the most important and critical issues. The first sample of information security that is being applied ever since mankind has existed, is encryption. The fact that the encryption has been being used since the early days of the history is an indication that the importance of the encrypted information is being awared. Encryption is not only a method used in the past. Today, it keeps its importance increasingly in terms of information security as well.

While the network devices are generally programmed over serial port (COM-RS232), communication is done without any password. The communication that needs to be done in order to secure the communication is an encrypting process with a strong encryption algorithm. When the communication is encrypted, even if an intervening hacker intervenes the communication, since the information obtained will be encrypted, it will not work.

For this purpose, the hardware system below is designed and the communication over the serial port is encrypted by using RSA encryption algorithm.

2. What is information and information security?

It means that on the computer networks and systems, the perpetually accessible information is transmitted confidentially from the sender to the recipient without any unauthorized or unauthorized access, alteration, disclosure, removal, tampering or damage.

As our individual and societal dependence on information systems increases, so will our sensitivity to the failure and attack that might occur against these systems. As this sensitivity increases, as a result of attacks that will be carried out against computer systems and networks; the loss on money, time,

Online ISSN 2603-459X

prestige and valuable information will increase as well. In case these attacks are directed to systems that directly affect life, such as hospital information systems, even human lives might be lost.

3. What are the network devices? How are they programmed?

A structured network is a network of interconnected computers for a variety of reasons, including information sharing, software and hardware sharing, centralized management, and ease of support. A wide variety of network devices can be used to create network configurations. The main devices used in networking are:

- Hub
- Switch
- Repeater
- Bridge
- Router
- Firewall devices (Firewall)
- Access point
- NIC (Network Interface Card)
- Modem

Network devices are usually programmed via the serial port (RS232) or over the network with the telnet protocol or ssh protocol. Communication process over the serial port is performed unencrypted.

3.1. Serial Port – RS232

Serial ports take their names from fact that the data via the port are sent in a rapid way namely they are sent a single bit at a time. The reason for this is that the port has its own single data line for all directions . Serial ports are also called COM ports. Because it creates a means of communication between external devices and the PC. The most common devices connected to serial ports are serial writing devices such as modems, mouses, printers, and plotters. The serial ports of the connectors are in 2 types. 25 and 9 pin. When you need to connect a 25-pin device to a 9-pin port or a 9-pin device in a 25-pin device, there are adapters that can be used in such situations.

Serial ports use two-level (dual) signaling thus the data rate in bits per second is equal to the symbol rate in the baud. The common bit rates per second used for asynchronous communication start/stop are 300, 1200, 2400, 9600, 19200 baud, and so on.

The speed of the connection point and the speed of the device must match each other. Frequently supported data rates; 75, 110, 300, 1200, 2400, 4800, 9600, 19200, 38400, 57600 and 115200 bit/s[1].

4. Encryption (Cryptology)

The secure transmission of information, ie the protection of the confidentiality and integrity of information during transmission, has become an important requirement. In particular, e-commerce and e-government projects, military, private and official writings via the internet, national security, internet banking etc. various algorithms and hardware and software that use them have been developed to ensure the security of information. As it can be understood from the applications we come across in daily life, when information security is said, encryption and decryption algorithms come to mind. Encryption is the transformation of a data into a form that is almost impossible to read without a proper information. The reason for this is to ensure the confidentiality of information from the people that we don't want information to be captured by, even if they try to reach the encrypted database Decryption is the opposite of encryption; is to recreate the encrypted data into a form that can be retrieved [2].

Encryption and decryption process usually requires the use of a secret information, known as "key". In some mechanisms, the same key is used for both encryption and decryption; while in other mechanisms different keys are used in both processes.

5. RSA Algorithm

The RSA algorithm, created by Ron Rivest, Adi Shamir and Leonard Adleman in 1977, is named after the first letters of the surnames of the developers. RSA which is an Encryption technique with a general key, was considered over creating very large integers and the difficulty of processing these numbers.. A more secure structure has been created by using prime numbers for key generation process . The reason for key generating by using the multiplication of two prime numbers is because, dividing the prime multiplication of two prime numbers into prime factors is more difficult than separating non-prime numbers [3].

In the RSA cryptosystem, key generation is done by the party that wants to receive the message. By generating public and private keys, the public key is made publicly available for everyone's use. A person who wants to send a message to this person uses this public key to encrypt the message he/she has and send it to the other party. The recipient of the encrypted message decrypts the encrypted message and obtains the original message using the private key it has generated. Let's examine the key generation, encryption and decryption steps below.

The key generation algorithm is as follows:

- Two very large prime numbers such as p and q are selected.
- The multiplication of these two prime numbers n = p.q and the missing ones φ (n) = (p-1). (Q-1) is computed.
- A prime integer e is selected between small φ (n) smaller than 1 and φ (n).
- The selected integer e is inverted in mode φ (n), the result is an integer such as d.
- e and n are the general keys, and d and n are the private keys.

After generating public and private keys, the information that wants to be sent is encrypted with the public key.

The Encryption process is done as follows:

- The party who will send the information obtains the general key e, n' of the receiving party
- The open text is converted to an integer as it will be the element M [0, n - 1].
- Encrypted text is computed as C ≡ M ^ e mod n.
- The sender of the information sends the encrypted text C to the receiver

Decryption process:

Using the private key of the receiving party obtains the open text as M ≡ C ^ d mod n again [3].

6. Developed System

The When communication with Serial Port (COM-RS232) is encrypted using RSA encryption algorithm, the system designed below is developed.

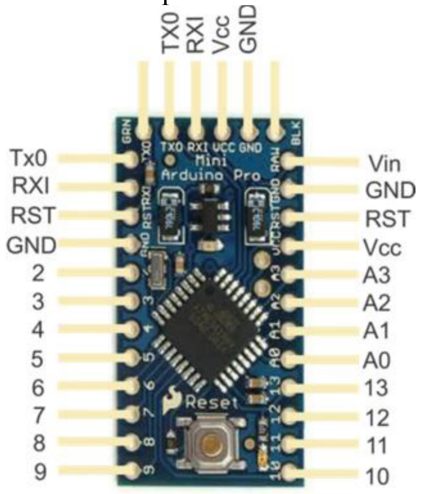


Figure 1. Arduino Pro Mini

Arduino Pro Mini Atmega 328, LCD display[4] and box were used as hardware system. All ascii characters [5] between 0-255 are encrypted with RSA encryption to create a look up table (LUT) table. Although the processing capacity of the used hardware was 8 bits, 16 bit encryption was done. Serial port communication was encrypted by Arduino software [6], the communication between was secured.

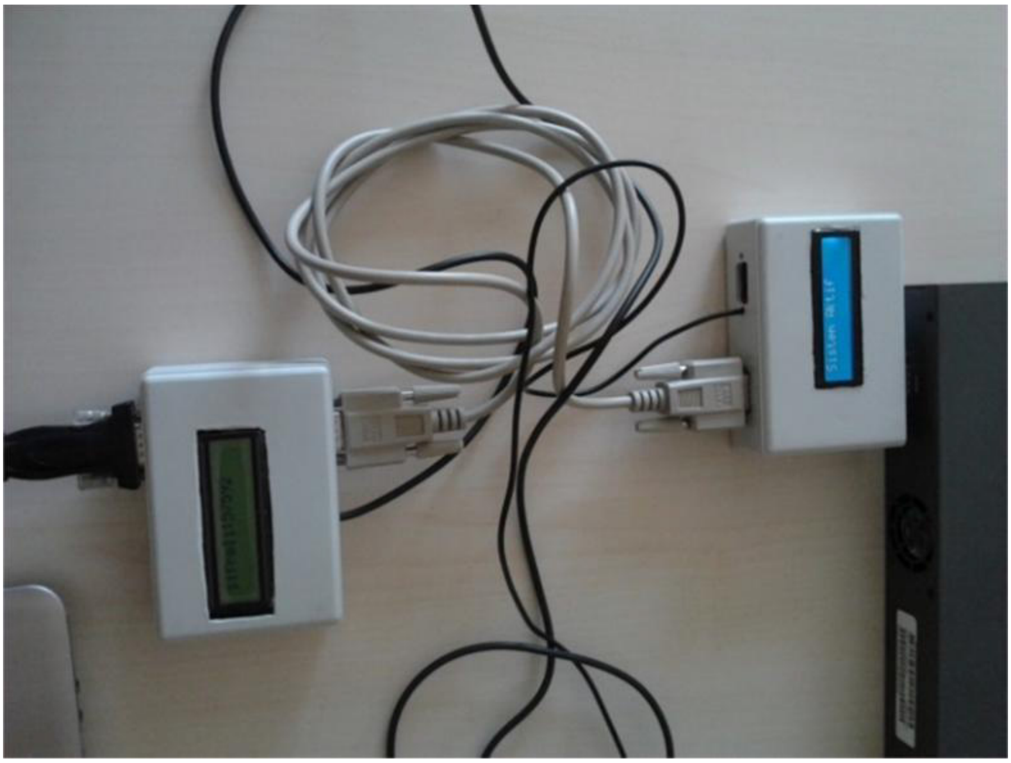


Figure 2. Developed Hardware System

The obtaining of 3316 which is encrypted by RSA, decimal value of 65 in the generated table was shown below in Figure 3. With the same method, all decimal values from 0 to 255 are encrypted with the CrypTool software and the table in Figure 3 is generated. Our system was designed by transferring the generated values shown in this table, in Arduino Pro Mini of our hardware. Since the encryption process has already been performed and the encrypted results are loaded in Arduino, there is no delay in serial communication.

Key generating process,

- Two prime numbers, p = 211 and q = 233 were selected.
- The value of n = p.q = 211x233 = 49163 was calculated.
- φ (n) = (p - 1). (q - 1) = 210x232 = 48720 was found.
- A random number e = 2 ^ 16 + 1 = 65537 which provides the condition of, φ (n) relatively prime with 1 <e <φ (n), was chosen.
- d = 44273, which provides the equivalence of 1 <d <φ (n) and e.d ≡ 1 mod φ (n), was found.
- The open key of the party receiving information became e = 65537, n = 49163 secret key became d = 44273, n = 49163.

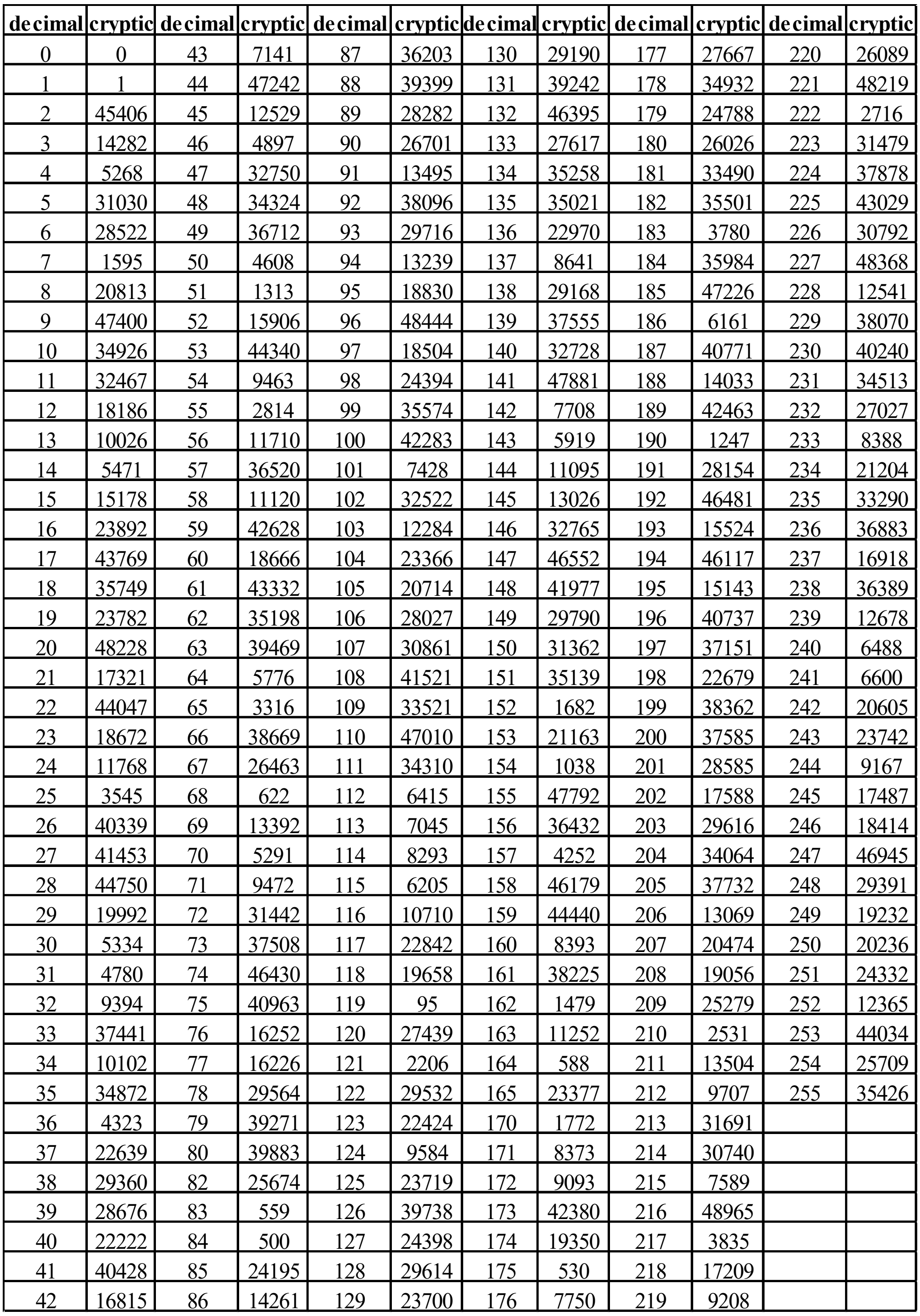
The encryption process,

- The party, receiving the information sends the open key e = 65537, n = 49163 numbers to the sender of the information via a channel open to the public.
- The open text of the side that will send the information was M = 65.
- The party that will send the information, calculates the encrypted text number C = 3316 which provides the equivalence C ≡ 65 ^ 65537 mod 49163

- The party sending the information, sends the number C = 3316 to the receiver of the information via a channel open to the public.

Decryption process,

- The open text 65 is obtained by computing the number M that provides the information receiver side M ≡ 3316 ^ 44273 mod 49163 equivalence.



de cimal	cryptic	de cimal	cryptic	de cimal	cryptic	de cimal	cryptic	de cimal	cryptic	de cimal	cryptic
0	0	43	7141	87	36203	130	29190	177	27667	220	26089
1	1	44	47242	88	39399	131	39242	178	34932	221	48219
2	45406	45	12529	89	28282	132	46395	179	24788	222	2716
3	14282	46	4897	90	26701	133	27617	180	26026	223	31479
4	5268	47	32750	91	13495	134	35258	181	33490	224	37878
5	31030	48	34324	92	38096	135	35021	182	35501	225	43029
6	28522	49	36712	93	29716	136	22970	183	3780	226	30792
7	1595	50	4608	94	13239	137	8641	184	35984	227	48368
8	20813	51	1313	95	18830	138	29168	185	47226	228	12541
9	47400	52	15906	96	48444	139	37555	186	6161	229	38070
10	34926	53	44340	97	18504	140	32728	187	40771	230	40240
11	32467	54	9463	98	24394	141	47881	188	14033	231	34513
12	18186	55	2814	99	35574	142	7708	189	42463	232	27027
13	10026	56	11710	100	42283	143	5919	190	1247	233	8388
14	5471	57	36520	101	7428	144	11095	191	28154	234	21204
15	15178	58	11120	102	32522	145	13026	192	46481	235	33290
16	23892	59	42628	103	12284	146	32765	193	15524	236	36883
17	43769	60	18666	104	23366	147	46552	194	46117	237	16918
18	35749	61	43332	105	20714	148	41977	195	15143	238	36389
19	23782	62	35198	106	28027	149	29790	196	40737	239	12678
20	48228	63	39469	107	30861	150	31362	197	37151	240	6488
21	17321	64	5776	108	41521	151	35139	198	22679	241	6600
22	44047	65	3316	109	33521	152	1682	199	38362	242	20605
23	18672	66	38669	110	47010	153	21163	200	37585	243	23742
24	11768	67	26463	111	34310	154	1038	201	28585	244	9167
25	3545	68	622	112	6415	155	47792	202	17588	245	17487
26	40339	69	13392	113	7045	156	36432	203	29616	246	18414
27	41453	70	5291	114	8293	157	4252	204	34064	247	46945
28	44750	71	9472	115	6205	158	46179	205	37732	248	29391
29	19992	72	31442	116	10710	159	44440	206	13069	249	19232
30	5334	73	37508	117	22842	160	8393	207	20474	250	20236
31	4780	74	46430	118	19658	161	38225	208	19056	251	24332
32	9394	75	40963	119	95	162	1479	209	25279	252	12365
33	37441	76	16252	120	27439	163	11252	210	2531	253	44034
34	10102	77	16226	121	2206	164	588	211	13504	254	25709
35	34872	78	29564	122	29532	165	23377	212	9707	255	35426
36	4323	79	39271	123	22424	170	1772	213	31691		
37	22639	80	39883	124	9584	171	8373	214	30740		
38	29360	82	25674	125	23719	172	9093	215	7589		
39	28676	83	559	126	39738	173	42380	216	48965		
40	22222	84	500	127	24398	174	19350	217	3835		
41	40428	85	24195	128	29614	175	530	218	17209		
42	16815	86	14261	129	23700	176	7750	219	9208		

Figure 1. Encoded ascii characters with RSA (generated LUT table)

7. Results

Today, communication between individuals, institutions and organizations via multiple computers is carried out in an electronic network environment. Given that any problem that may arise in this large electronic networking environment can affect the entire network in a negative way, data security will become more important today [7].

Transferring data from one point to another in a network environment is realized using different technologies. Network devices used during communication are also under threat like computers. These devices can also be listened easily by the softwares which listen the entire network.

When data is being sent to any organization or person via computer networks, the data is transmitted to the target computer over one or more computers. The confidentiality and integrity of the data must be preserved during transmission of the data to the other party through many computers and network equipment. It is now important to control the network devices used and to manage them in accordance with certain policies as they are in computers. Security of the computer networks must be provided with enterprise information security approaches and preventive software and hardware should be used to ensure security.

References

[1] Lovine J 2012 *PIC Projects for Non-Programmers* (USA:Elsevier) chapter 8 pp 151-187

[2] Stinson D R 2002 *Cryptography: Theory and Practice Second Edition* CRC Press

[3] Schneier B 1996 *Applied Cryptography Second Edition* (New York: John Wiley & Sons Inc)

[4] Lovine J 2012 *PIC Projects for Non-Programmers* (USA:Elsevier) chapter 7 pp 115-149

[5] Ascii table *http://www.asciitable.com/*

[6] Arduino software *http://www.arduino.cc/en/Main/ Software*

[7] Canberk G and Sagıroglu S 2006 *Bilgi ve Bilgisayar Güvenliği Casus Yazılımlar ve Korunma Yöntemleri* (Ankara: Grafiker Ltd. Şti.)