



"HENRI COANDA" AIR FORCE ACADEMY
FACULTY OF AERONAUTICAL MANAGEMENT
OMANIA

STUDENTS' INTERNATIONAL CONFERENCE AFASTUD 2015
Communicating Across Cultures
Brasov, 2nd-4th April 2015



"GENERAL M.R. STEFANIK"
ARMED FORCES ACADEMY LIPTOVSKY MIKULAS
SLOVAK REPUBLIC

CREATING A CRYPTO DEVICES AND ITS APPLICATION

cad. Péter Szegedi

Faculty of Military Sciences and Officer Training, National University of Public Service, Budapest, Hungary

Abstract: The topic of my article is a project, made for our University's scientific student conference. Its purpose is to create a crypto device capable of providing secure communication between two points. Differently, from governmental devices, the goal was to use cheap resources, open source software, easily taught and learned techniques. It aims to be used as an experimental device.

Keywords: Raspberry Pi, cryptography, programming, networks, Python

1. INTRODUCTION

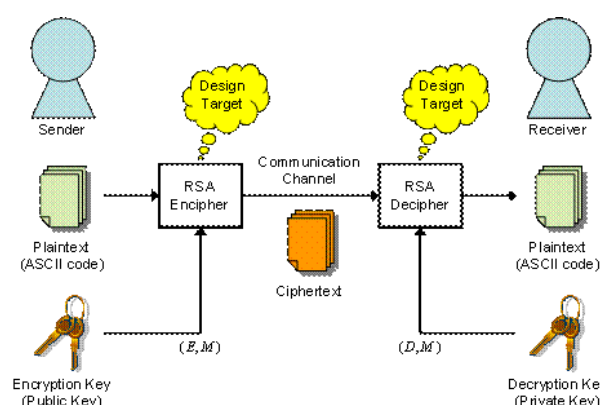
In today's society our information's security, our privacy are both key concepts. Since recent events, like the Snowden scandals, when people found out about NSA's involvement in public espionage, or the so called Heartbleed, a major flaw in the well-known SSL/TLS protocol, people became aware of the IT security generally.

In my topic, I'm mostly involved in cryptography, which is basically the science of secure communication. I wanted to know, what are the possibilities, to create secure communication using a crypto device? Of course, there are specific hardware created by official authorities, but my research was about implementing such a device at home conditions, with basic equipment.

2. CREATING THE CRYPTO DEVICE

2.1 The algorithm. Creating a crypto device is a complex process, which requires some knowledge from various fields. First of all, mathematics is necessary to understand cryptographic functions, which are the background of the process created. Technically one's privacy is as strong as the cryptographic

algorithm used for the encryption. For this project, it is necessary to use such a method, which is generally accepted as secure nowadays. There are various algorithms available, and my choice was one, which can be considered a classic now, the famous RSA (named after the authors, Rivest, Shamir, Adleman), with sufficiently strong key (2048 bits).

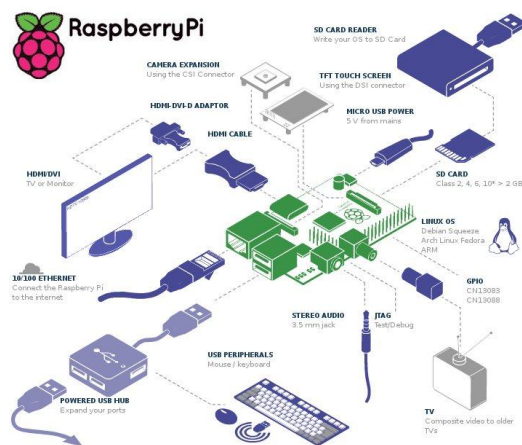


1. figure: RSA working in theory

2.2 The device. For creating a secure line of communication I needed at least two devices which are involved in it. It is possible to use a standard PC, but to make it more specific and cost-effective, I chose something different. In the IT world, day after day, the so

called Raspberry Pi becomes more and more famous. Technically it is a fully built-up PC, with all the peripheral inputs which are expected to be in a modern computer. The inside parameters are a bit behind today's top notch laptops and gamer PCs, but maximally useful, for experimental or research projects (although its preferences differ by version).

What makes it special is its size, technically not larger than a credit card. This makes it much cheaper than classical PCs (new A+ versions are available for 20\$), makes it portable and comes with low energy usage. Altogether it makes a perfect choice, for building up a crypto device from zero.



2. figure: I/O possibilities for Raspberry

Apart from its physical attributes, it is necessary to mention the operating system as well. It basically comes with a Linux Debian distribution, specially created for the device, called Raspbian OS. It is open source, easily installed, and perfectly fitted, which makes it optimal for beginners. One extra preference made it especially useful for the project, its full support of the Python programming language, which I will describe later.

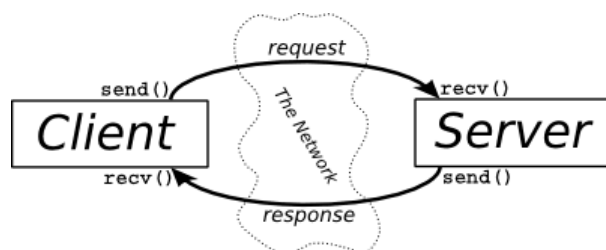
2.3 The network configuration. Finding a suitable device was an important step, but I had to figure a way to connect the two of them, to establish the communication. Since it supports a standard UTP cable input, one possibility was to directly connect them with a cross link cable. Since the Raspberry doesn't come with I/O devices, controlling them through the network would be more useful, as well as more technical. Also it was better for

simulation, therefore I created a small network, consisting of the two devices, a switch, and a "master" PC for control. This would then represent, even in small forms, a communication going through a network.

Controlling the devices was the next challenge, since it needs some technical skills. Fortunately, Raspbian fully supports SSH (Secure Shell), which is an ideal way to create a connection with a command line interface. With a little IP configuring, the devices were ready for the messaging, all they needed was the software background for it

2.4 Programming. The last part of setting up the system is the one requiring the most IT skills. My idea was, when creating this project, to be easily applied by other enthusiastic students, who want to experiment with applied cryptography. This is why I chose popular, available and open source devices and software (Raspberry Pi, Raspbian OS, SSH), and this is the reason for choosing Python as programming language. It is easily learned, considered to others, yet powerful, not to mention its enormous online support community.

Given the programming language, I started with building up the network connection (software part of it), by using socket module. It is implemented in the language, and it was created especially for establishing connection between devices for the purpose of message based communication. Therefore setting it up with the proper configuration created a device which is constantly "listening" for incoming (UDP) packets, while the other side sent these, then they switched.



3. figure: Rough overview of socket

One extra addition has to be mentioned, the system uses infinite loops to constantly send useless messages (which seem encrypted for a third party), to make it harder to even spot the



"HENRI COANDA" AIR FORCE ACADEMY
FACULTY OF AERONAUTICAL MANAGEMENT
OMANIA

STUDENTS' INTERNATIONAL CONFERENCE AFASTUD 2015 *Communicating Across Cultures*

Brasov, 2nd-4th April 2015



"GENERAL M.R. STEFANIK"
ARMED FORCES ACADEMY LIPTOVSKY MIKULAS
SLOVAK REPUBLIC

actual message (which has to be decrypted also, for an ill-wisher).

Of course sending packages across a network is nothing special, not to mention the lack of cryptography. For that purpose, comes in a very useful module package for Python, called PyCrypto, which is open source, and contains all relevant cryptographic algorithms implemented.

This way I started with generating the key pairs (public and private) required for the encryption process. Using the key pairs with the RSA method gives a fine encryption, but to make it more specific, I implemented a digital signature. This way, a message, above being encrypted, can be validated if it actually does come from the source it should be coming from. For this purpose, I made a hash (using MD5 standard) of the message, and implemented a signature on it, with the exchanged keys. Now the plaintext can be encrypted also with the created secret key, and be sent together with the signature. The second party receiving it decrypts the message as well as checks the signature, if it is valid or not.

Of course, the whole process mentioned above is done automatically through an executable file, only for the topic of this material I went into details of the implementation. To come as user friendly as possible, it displays incoming messages, and gives opportunity for an input, as well as automatically creates a log file of the communication.

3. CONCLUSIONS & ACKNOWLEDGMENT

Creating and implementing a fully working crypto device was a project that required skills

from multiple areas. As a conclusion, it has to be said, that in all areas, but especially in military, the need greatly arises for security. More and more people come in contact with more and more sensible data throughout their jobs, and great resources are applied for the use of cryptography, which is praiseworthy, yet it seems, there are alternatives, and ways for improvement. The use of smaller devices create a better opportunity for the device storage, which is strictly regulated, in case of crypto devices, especially under military usage. Not to mention the cost reduction and other useful benefits which comes with it (considerably smaller power source, easier cooling, or replacement in case of malfunction, etc...).

It would be foolish to say, that the created device (system) in its current state is fully suitable in military life, for a 100% secure communication. This is more like a basic idea, a new way for future development, not to mention its educational purpose, as I think many are eager for a DIY (Do It Yourself) solution, and would like to have a practical use of their networking or programming skills.

BIBLIOGRAPHY

1. Bruen, Aiden A. & Forcinito, Mario A.: Cryptography, Information Theory, and Error-Correction: A Handbook for the 21st Century. John Wiley & Sons, 2011
2. Wobst, Reinhard: Cryptology Unlocked. Wiley. 2001
3. Buttyán Levente – Vajda István: Cryptography and its application, Typotex, 2004
4. Sean McManusm, Mike Cook: Raspberry Pi For Dummies, John Wiley & Sons, 5.