Block diagram and Flowchart for EE an CS roles

TEAM 3

Introduction

Secure Messaging and Location Tracking project can be called as a messenger program being run on smart phones (Android operating systems) and having the feature of enabling users to see the positions of each other on a map. All the information shared within the group is encrypted.

In this project, a portable cryptographic device which encodes the data sent from the mobile device will be designed. Public key encryption with RSA Algorithm will be used. The connection between the cryptographic device and mobile phone is done through Bluetooth technology.

A user interface which displays the locations of the other users on a map is designed. The location information is read from the integrated GPS chip inside the smart phone. Obtained coordinates are interpreted and users are demonstrated on the map with symbols. This user interface also enables the user to send and receive encrypted messages via this application. Together with the location information, the plaintext is sent to the cryptographic device via Bluetooth. Encrypted information is transmitted to the other users via a HTTP Server application.

The received and transmitted messages are stored during the session. Last few locations of the users are also stored internally in the program in case of a GPS or Internet connection loss. In such unexpected emergency cases, other users who still have the connection can reach the last location of the user who has lost his connection.

Hardware Block

The hardware part consists of two main blocks which are Bluetooth Transceiver (BT) and Encryption/Decryption (D/E).

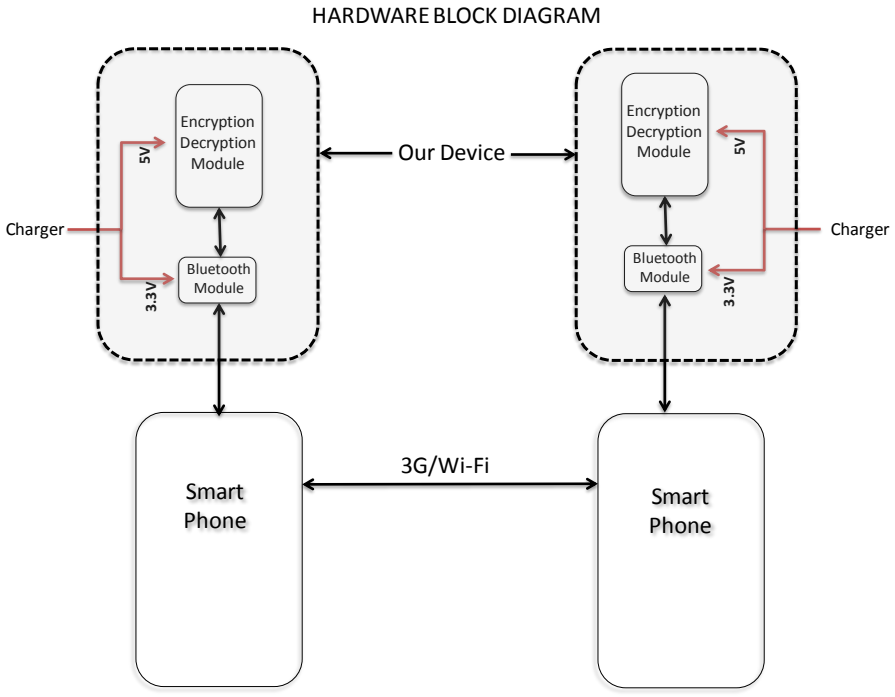


Figure 1 – Hardware Block Diagram

The data (short message or location of the user) is transmitted from the phone to the D/E Block via Bluetooth connection. If this information comes from other users (PersonB or PersonC), it is sent to D/E Block for decryption. The plaintext is transmitted to phone after decryption again via Bluetooth connection. If this information is created by the user (PersonA) to be sent to other users (PersonB and PersonC), it is transmitted to D/E Block for encryption. The ciphertext is transmitted to phone after encryption again via Bluetooth connection. Figure1 visualises this process.

An encrypted message can only be decrypted by a private key. It can be encrypted by the public key. Description of a messaging network where Person A sends his position, Person B and Person C receives his position. Person A encryptes his position by using the public keys of Person B and Person C. In other words, a different encryption is implemented for each user. Person B and Person C receive this information and decrypt it by using their private keys. The keys are created and exchanged when a user is logged on the program. Therefore, three different modes can be defined for D/E block which are Key Generation, Decryption and Encryption. These modes are explained under Encryption/Decryption Block heading.

Encryption/Decryption Block

In conventional secret key cryptographies, the recipients and senders share the encrypted information within a small group. The key is single and it is known by the every user of the network. In other words, each user has to trust each other on the secrecy and the protection of the key [1]. Public key encryption is an asymmetric algorithm which is based on the use of two keys: private and public. This difference from the symmetric algorithms can also be regarded as its superiority. Each user protects the secrecy of own private key. Due to these reasons, public key encryption has become a fundamental and widely used technology [2].

RSA Algorithm is first invented in 1977. It pioneered to the development and proliferation of the public key algorithm. In this project, RSA Algorithm method is chosen since it is the most widely-used public key algorithm [3] and extensive research [4], [5], [6] and [7] which has been made on RSA Algorithms and their hardware implementations can be reached.

It has been decided that the hardware implementation of the Public Key algorithm is done on FPGA Chips. FPGAs offer two important advantages: Flexibility and Integration [8]. With the same circuitry and connections, the implementation of different encryption algorithms can be realised. Different implementation methods of RSA Algorithms on FPGAs are also widely researched [9] and [10].

In this project, the cost of the FPGA Chip is an important constraint on hardware designers. It has been experimented that RSA encryptions which can perform up to 1024-bit encryptions operations can be implemented on FPGA chips by using less than 14K logic elements at 17.77 MHz clock frequency and less than 1us [9]. In this project, short messages and location information will be encrypted. The size of the data is small. Therefore, the speed performance is not the primary concern. Therefore, low cost FPGAs in the market are examined. Different candidates are given below [11]:

- Altera:

EP1C3T100C8N – Number of LEs: 2910 and Cost is 10.70 US Dollars.

EP1C6T144C8N - Number of LEs: 5980 and Cost is 17.50 US Dollars.

EP1C12Q240C8N – Number of Les: 12060 and Cost is 35.50 US Dollars.

EP1K10TC100-3 – Number of Les: 576 and Cost is 4.95 US Dollars.

- XILINX:

XC2S50-5TQG144C - Number of Les: 1728 and Cost is 12.85US Dollars.

XC2S100-5TQG144C - Number of Les: 2700 and Cost is 17.60US Dollars.

XC3S500E-4PQG208C - Number of Les: 10476 and Cost is 27.60US Dollars.

As a modest choice, ALTERA EP1C3T100C8N has been chosen as the FPGA Chip of in this project. However, if higher encryption performance is required, advanced FPGA models with high number of logic elements can also be considered. In Business Plan, the price of this chip is considered. In Product Requirements Report its size is taken. In the first semester, it is targeted to implement the project on Spartan 3E Development Kit since the hardware engineers already have it and are used to it. Spartan3E FPGAs are superior to the FPGA chips which are presented above; however, they are more expensive. According to the experiences gained in the first semester, the choice of the FPGA Model can be reconsidered.

Encryption Block Diagram

RSA key generation algorithm can be summarised as below [4]:

1. Obtain p and q which are distict large random primes.
2. Calculate modulus n = p x q.
3. Calculate Euler's totient function Phi(n) = (p-1)(q-1)
4. Select integer e within (1, Phi(n)) range. Note that gcd(Phi(n), e) = 1.
5. Calculate d = e^{-1} mod Phi(n) (d is private exponent).
6. PUBLIC Key can be published as (e,n).
7. PRIVATE Key can be kept as (d,n).

RSA Encryption algorithm:

1. Plaintext M has been defined.
2. Ciphertext C can be created using public key: C = M^e mod (n).

RSA Decryption algorithm:

1. Ciphertext C has been received.
2. Plaintext M can be obtained using private key M = C^d mod(n).

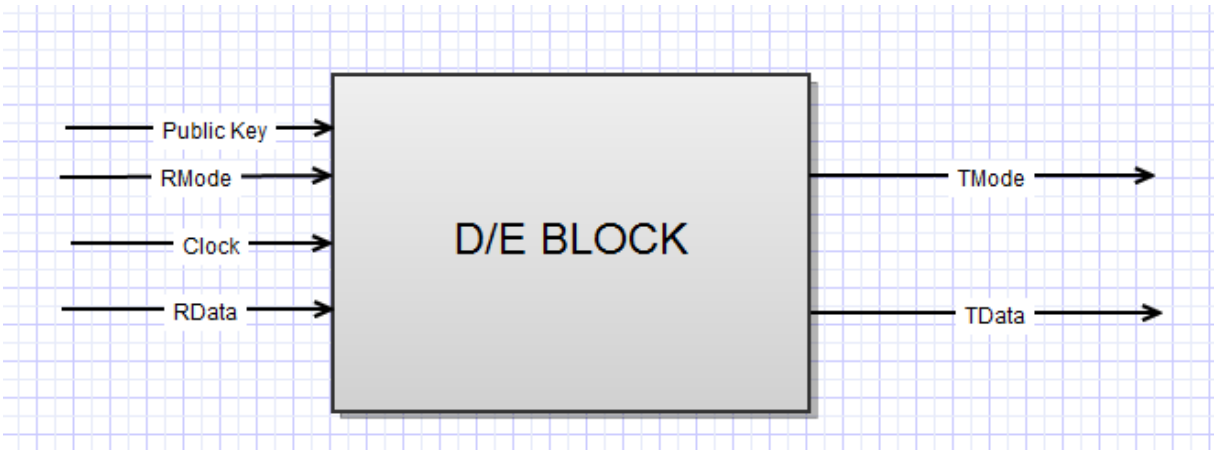


Figure 2 - I/O Relation of D/E Block

Inputs/Outputs:

- “Public Key” is necessary to encrypte a data which will be transmitted.
- Rmode indicates that a data is at the input of D/E Block and its purpose. Received data (RData) can be ciphertext or plaintext. If it is ciphertext (plaintext), than D/E Block works in decryptor (encryptor) mode.
- Clock signals are used in VHDL Programming. In this case, random number generation module also uses clock signal.
- Tmode indicates that a data is at the output of D/E Block and its purpose. Transmitting Data (Tdata) can be ciphertext of plaintext.

Switch module takes single input which is the state of the hardware component. Switch creates an output ChoiceOfKeys with respect to RMode input. According to ChoiceOfKeys, either public key of Person B in order to encrypt a message written by Person A to be sent to Person B or private key of Person A in order to decrypt a message coming from Person B is sent to ModExp module. ModExp module simply performs modular exponentiation. Keys submodule also gives the public key of A to be sent to other users.

The block diagrams given above are not finalized yet. After discussion of possible issues, these block diagrams can be modified further:

- The challenging part of PKE implementation is the modular summation, exponentiation and multiplication efficiently and correctly.
- In this design, random numbers are generated by using a clock signal. A perfect random number creation should be theoretically an output of a physical experiment. Possible other hardware implementations such as deriving a random number from a temperature sensor can be discussed.

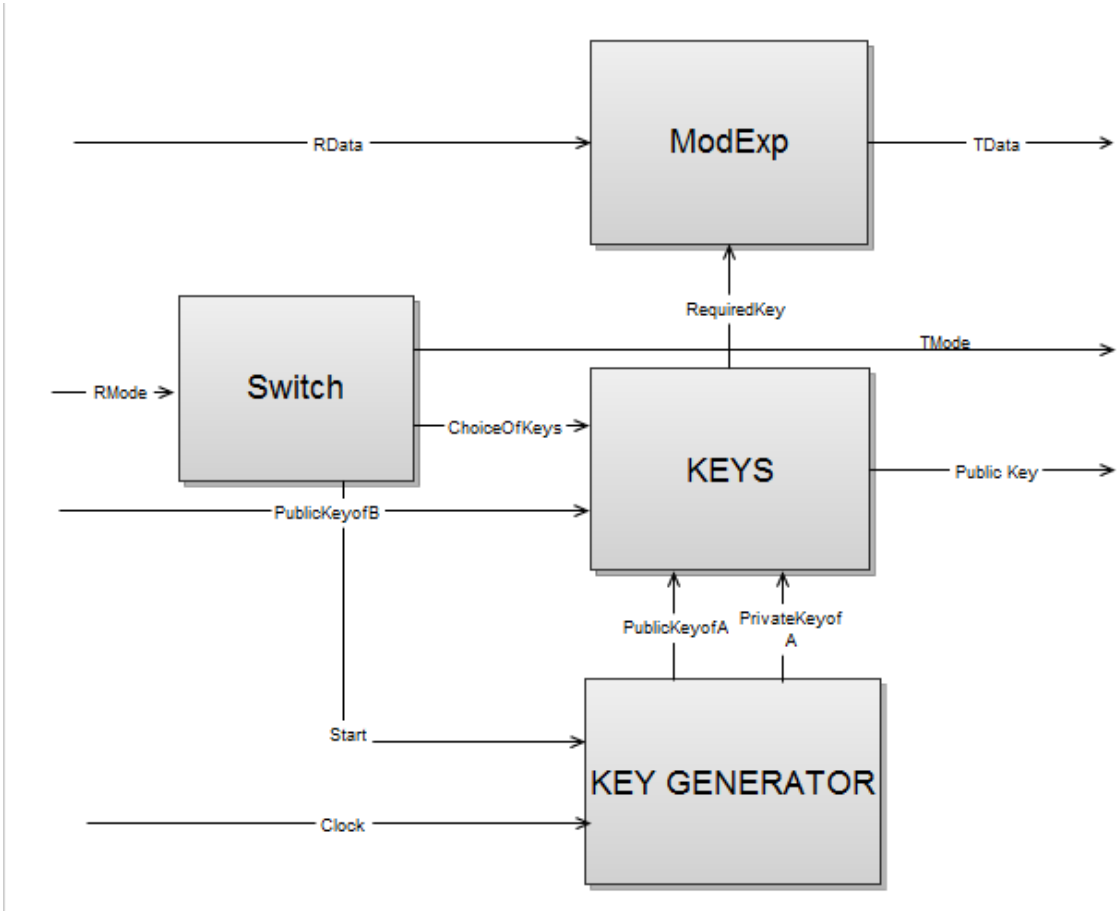


Figure 3 – D/E Block Diagram with SubModules

KeyGenerator Module is implements the RSA Key Generation algorithm which is given above. It gives two outputs which are public key and private key. KeyGenerator module is activated when information which belongs to Person A will be sent. KeyGenerator module is started by the Switch module.

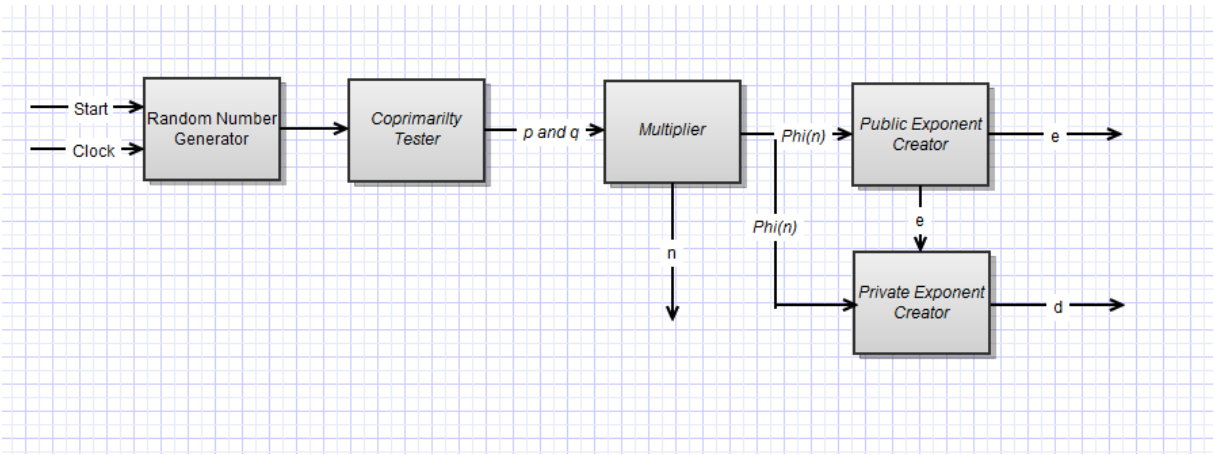


Figure 4 – Key Generator SubModule

Bluetooth Transceiver Block

The transceiver block receives the information which is the location of the user and message and sends it to the encryption block. The connection of D/E and Smartphone is done via this block. Even at the beginning of the project description, it has been decided that this block should be a wireless technology, because wireless technologies are portable and has specified standards. Between two widely-used wireless technologies which are Bluetooth and Wi-Fi, Bluetooth technology is chosen due to several reasons:

- Wi-Fi connection is generally used to connect to the Internet through a stationary access point. Bluetooth technology is designed to connect directly electronic gadgets [12]. In this project, wireless communication is needed to connect to D/E to Smartphone. There is no need to establish a local area network. Therefore, it is logical to choose Bluetooth technology due to its simplicity and efficiency in design and implementation.

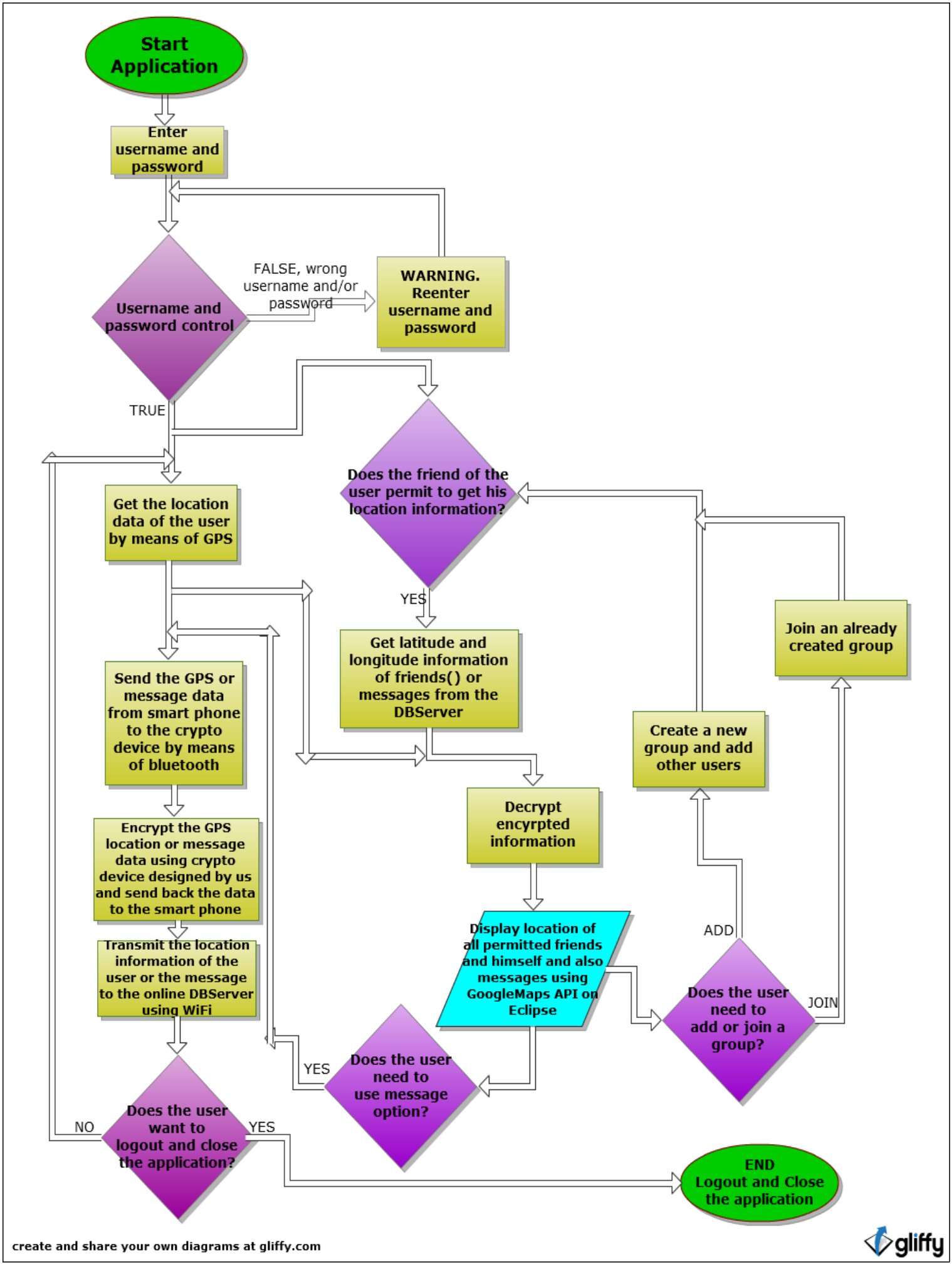
- For many users, it can be assumed that Wi-Fi connection of the Smartphone is busier than the Bluetooth device unless the user is communicating via a Bluetooth headset. It is more logical to use the free channel in this project.

- Bluetooth is more secure, offers less power consumption and has a shorter range. The range is the advantage of the Bluetooth technology in this case [13].

CC2540 Texas Ins. Bluetooth Transceiver is chosen since we already have its development kit. There are different versions of this model which have different packaging and memory size.

The unit price of this module varies around 4 US Dollars depending on its version.

Software FlowChart



Conclusion

With this block diagram and flow charts report, main building blocks of the system are defined. The next approach in the hardware development is understanding how Bluetooth module can be driven and implementation of the PKE on FPGA Board. In Fall Semester, Hardware group plans to physically finalizes the project on development kits level. We already have the Spartan IIIE and CC2540 Texas Ins. Bluetooth Development Kits. Therefore, the choice of FPGA Chip and Bluetooth Module can be alternated at the end of semester based on the experiences obtained from the development kit works.

References

[1] *"Introduction to Public Key Cryptography"* Last Accessed on 18.11.2011 *http://www.verisign.com.au/repository/tutorial/cryptography/intro1.shtml*

[2] "*Public-key cryptography"* Last Accessed on 18.11.2011 *http://en.wikipedia.org/wiki/Public-key_cryptography*

[3]*"RSA Algorithm"* Last Accessed on 18.11.2011 *http://www.di-mgt.com.au/rsa_alg.html*

[4]*"RSA Hardware Implementation"* by Çetin Kaya Koç.

[5] *"Hardware Architectures for Public Key Cryptography"* by Lejla Batina, Sıddıka Berna Örs, Bart Preneel and Joos Vandewalle.

[6] *"Flexible Hardware Design for RSA and Elliptic Curve Cryptosystems"* by Lejla Batina, Geeke Bruin-Muurling, and Sıddıka Berna Örs.

[7] *"Design and Implementation of an Improved RSA Algorithm"* by Yunfei Lİ, Qing Liu and Tong Li.

[8] *"Three Reasons to Use FPGAs in Industrial Designs"* Last Accessed on 18.11.2011 http://dkc1.digikey.com/us/en/tod/Altera/Reasons-To-Use-FPGAs_noaudio/Reasons-To-Use-FPGAs_noaudio.html

[9] *"FPGA Implementation of RSA Encryption Engine with Flexible Key Size"* by Muhammad I. Ibrahimy, Mamun B.I. Reaz, Khandaker Asaduzzaman and Sazzad Hussain.

[10] *"RSA & Public Key Cryptography in FPGAs"* by John Fry and Martin Langhammer.

[11] *"Digi-Key Corporation"* *http://www.digikey.com/?curr=USD*

[12] *"What is the difference between Bluetooth technology and Wi-Fi?"* Last Accessed 18.11.2011 http://www.bluetooth.com/Pages/Wi-Fi.aspx

[13] *"Bluetooth vs Wi-Fi General Comparison"* http://www.penmobile.co.uk/files/featuredarticles-filename-2.pdf