Crypto Algorithm

Md. Mahmudul Hasan Sumon

August 2018

Contents

1 Introduction

Security is a must have a feature in next version of VTS. As from previous study we found that providing TLS v1.3 over 2G network is troublesome. It require some number packet transaction at TLS handshake process to make the connection secure. After connection become secure normal data transfer occurs. So current version of VTS will not use TLS v1.3 implementation.

A simplified version of RSA encryption is considered to be used to provide security on VTS data. A lower key size is chosen. But security should not violate as the key is not fixed for a specific client. Rather key will generate on the fly based on two random prime number. A set of prime number will store from where two random number will chosen and key is generated. When connection is closed another new pair will be selected and new key will be generated.

2 RSA

RSA is asymmetric crypto algorithm. A key pair is used to encrypt and decrypt original data. It has public key and private key in its pair. Public key is used to encrypt message and private key is used to decrypt that massage.

3 Protocol

The proposed protocol consist of three operation.

* **Key generation:** Generate key using two 16-bit arbitrary prime number. Key size 32-bit.

* **Connection establish:** Establish connection between server and client. Share public key.

* **Data serialization:** Encrypt and serialize data to transfer so remote user can decrypt it.

3.1 Key generation

In the proposed protocol dynamic key is used. A single key pair is used for only once in a connection. When connection is closed from eith!her side a new key pair is used for data encryption. To provide this mechanism a key generation algorithm is used. Key is generated when connection is being made. A large collection of prime number is stored in array. Two prime number is choose from the array of prime number using random basis. These two prime number then used to generate key pair. After that public key is shared with server. Server also do the same during connection establishment. Below flowchart describe the step required to generate key pair.

3.1.1 Main algorithm

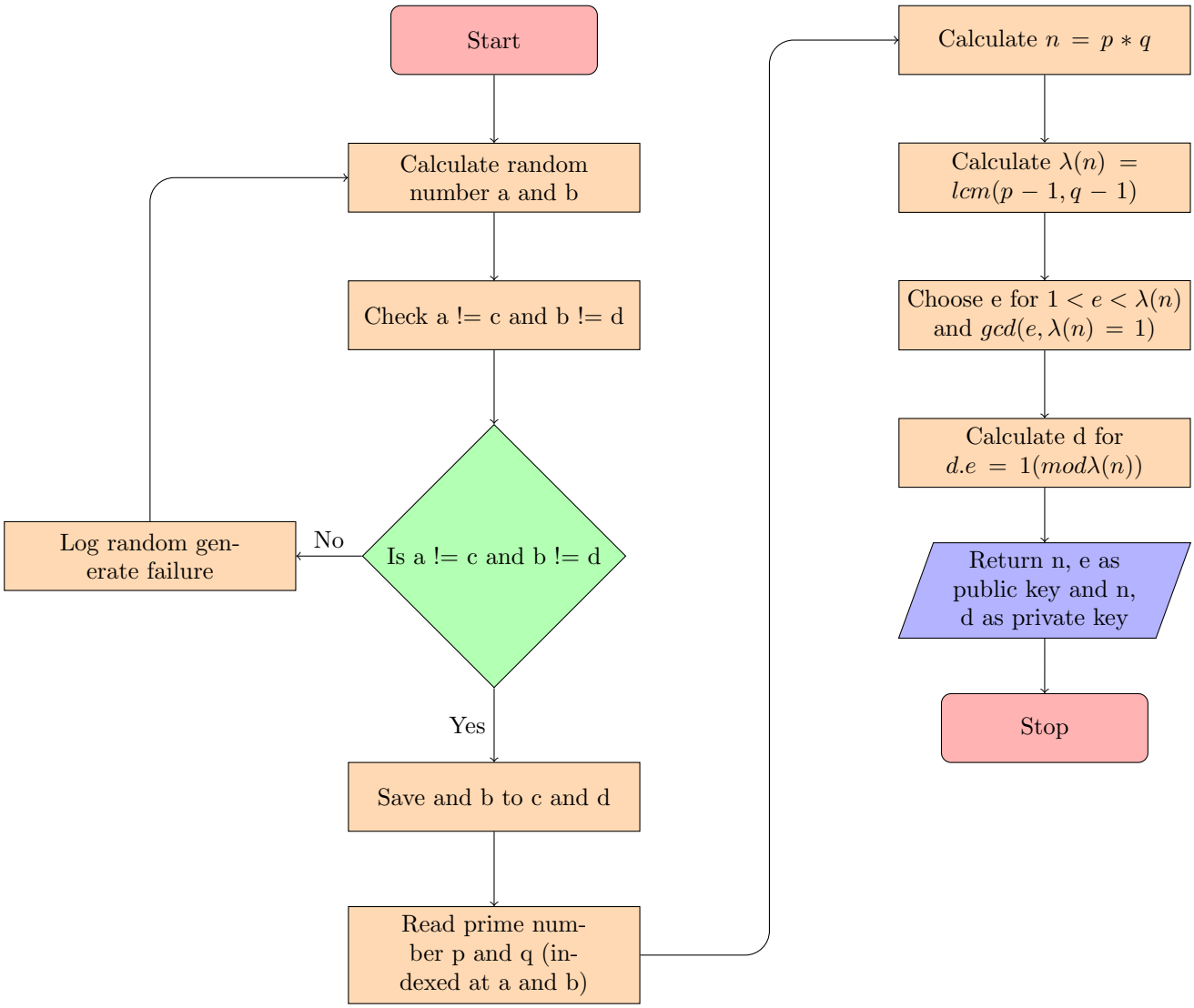

Figure 1: Key generation

3.1.2 Modular Exponentiation

To compute modular exponentiation of a number ($num^e \quad mod \quad m$), we use BigMod recursive algorithm.

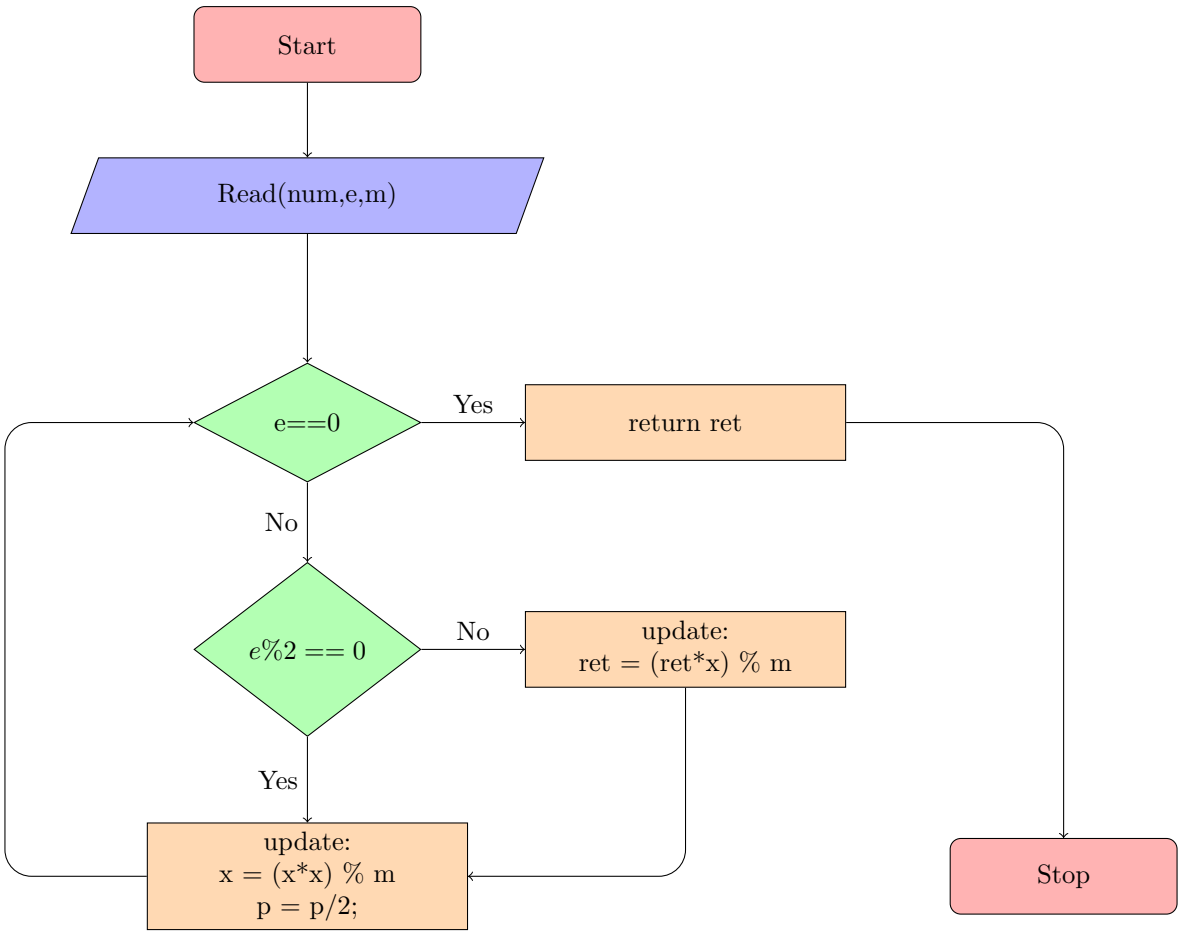

Figure 2: Modular Exponentiation