Barry's Linear Private Key and Public Certificate Exchange

By

Barry L. Crouse Ph.d Computer Information Systems

Table of Contents

Chapter 1 **Visual representation of Idea.**

Chapter 2 **Mathematical Formula and Process**

Chapter 3 **Development of Project and testing**

Introduction

I would like to begin by outlining a problem I have been continuing to see without any solutions. The Process I am proposing is what I have seen the last month during the holidays mainly Thanksgiving and Christmas 2016.

I have developed a Private Network with state of the Art Security and it has shown me some fundamental flaws in Certificates and Key exchanges. This Patent idea uses strictly Linear Based Motion incorporating Asymmetrical keys and passwords. The Specs for the type of System calls for a Low End Server 8 Gig of Memory to 16 Gig.

One of these problems was shown by a Financial Institution that used RSA 2048 Certificate that implemented TLS 1.1 but the key was obsolete dated back in 1999 over 17 years ago. A key is used to open the Certificate. When it is obsolete, The Certificate can easily be damaged or corrupted.

I will begin by proposing a Asymmetrical Key with 12288 RSA Regular 4096 with two sub-key Encryption at 4096 bringing the total to 12288 bits. The reason why it is not Symmetrical is because it would not be automated to copy the blocks or chunks of data on the clipboard because the UTF Character Encoding schemes along with bit and byte representation will be set differently not the standard UTF-8 bit schemes. Please note the RSA Certificate is 5120 PKCS12 with password protection and the 12288 key uses a different password not one size fits all mentality.

I will begin by providing the Charts and than provide the Process involved. The next chapter begins the Charts Visual Representation.

Chapter 1

Visual Representation of Idea

Barrys Scientific Based Products

End-User UTF Menu

1). Method 1.1 UTF-16

2). Method 1.2 UTF-32

3). Method 1.3 UTF-64

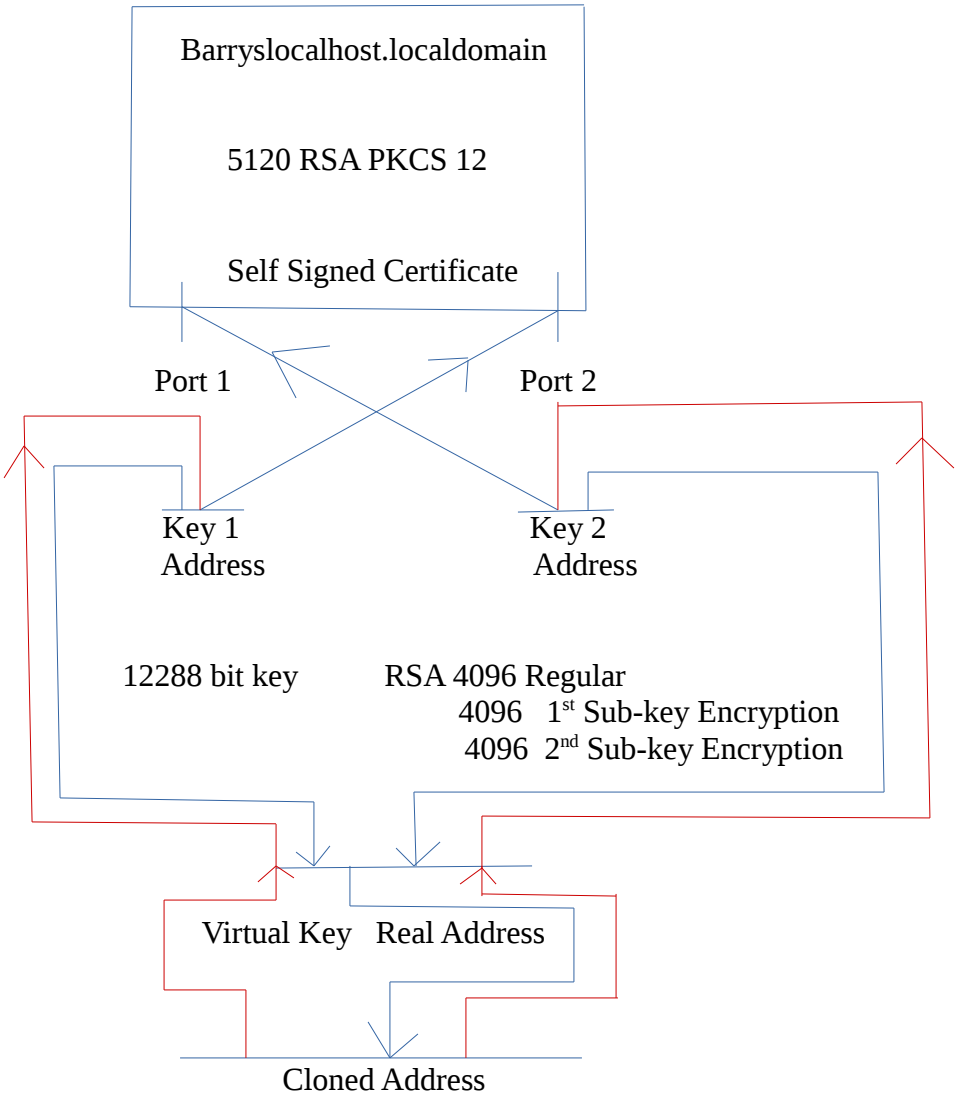
4). Method 1.4 UTF-128

Main module Psuedo Logic

```
If “1” goto Method 1.1
      else
if “2” goto Method 1.2
      else
if “3” goto Method 1.3
      else
If “4” goto Method 1.4
       else
          goto exit
         end
 Rem This is a sample main module on how the methods can be chosen by setting
 Rem       up a main module the methods show in great detail along with submenus
```

View 1 Character Encoding UTF-16 Bits

4 Bytes = 1 Character



Method -1.1

12288 * 12288 = 150994944 Bits

150994944 / 16 = 9437184 Bits

9437184 / 64 = 147456

√147456 = 384 Bits

384 / 4 = 96 Characters

Table of Character Fields

Barrys Scientific Based Products

User Real Time Mode Choice

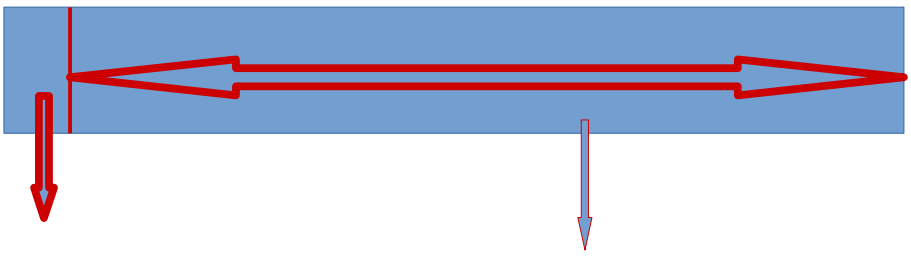
1). 96 / 12 = 8 Fields {+,-} X = Prime Number

2). 96 / 16 = 6 Fields {+,-} X = Prime Number

3). 96/ 24 = 4 Fields {+,-} X = Prime Number

4). 96/ 48 = 2 Fields {+,-} X = Prime Number

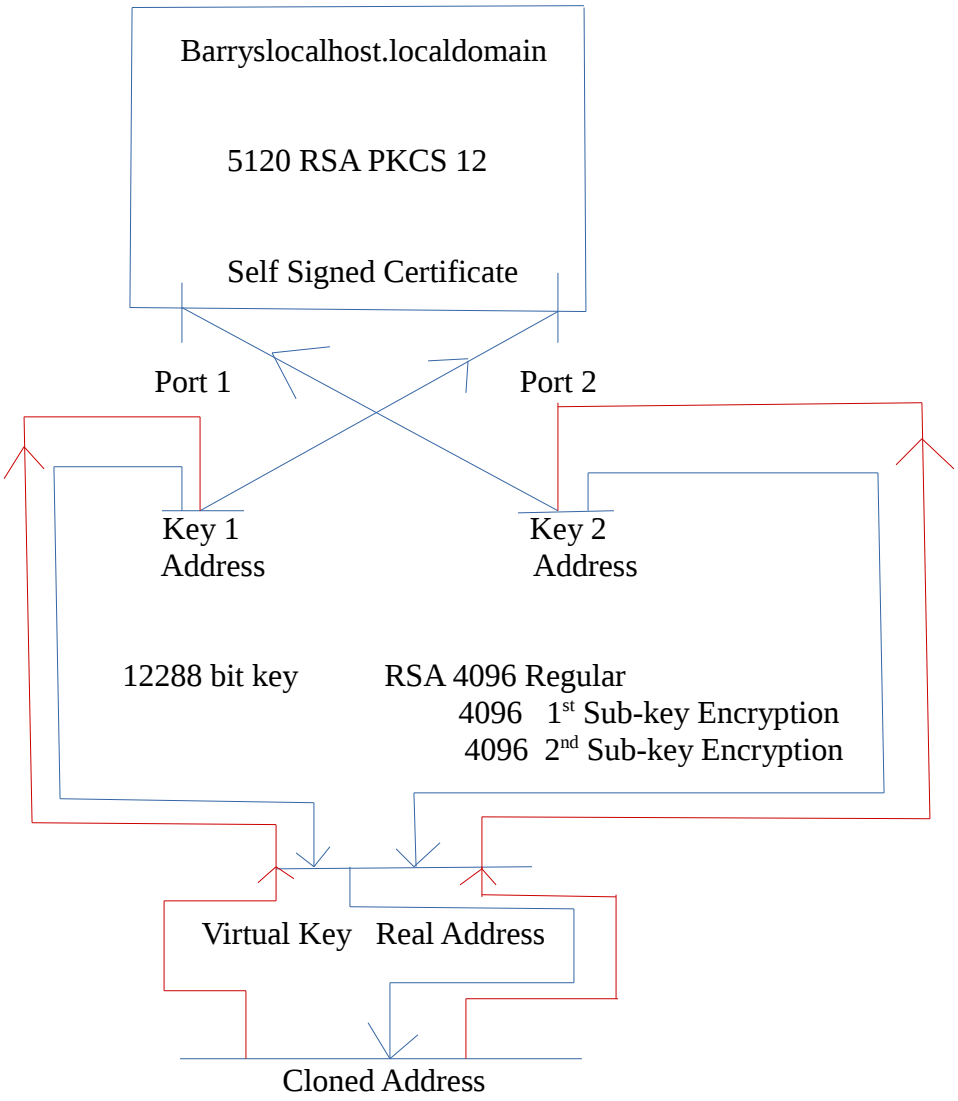
Data Block



Header Padded 96 Characters

View 2 Character Encoding UTF-32 Bits

4 Bytes = 1 Character



Method -1.2

12288 * 12288	=	150994944 Bits
150994944 / 32	=	4718592 Bits
4718592 / {32 bits * 4 Bytes} = 128	=	36864
√36864	=	192 Bits
192 / 4	=	48 Characters

Table of Character Fields

Barrys Scientific Based Products

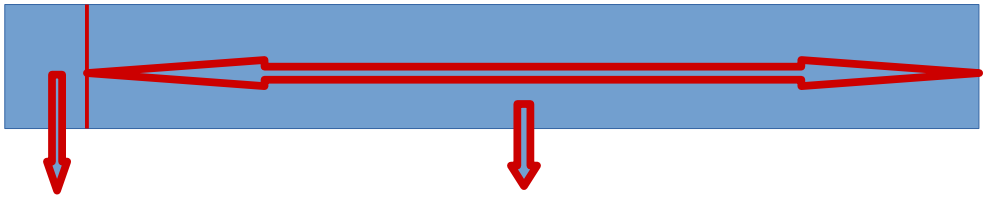
User Real Time Mode Choice

1). 48 / 8 = 6 Fields {+,-} X = Prime Number

2). 48 / 12 = 4 Fields {+,-} X = Prime Number

3). 48/ 16 = 3 Fields {+,-} X = Prime Number

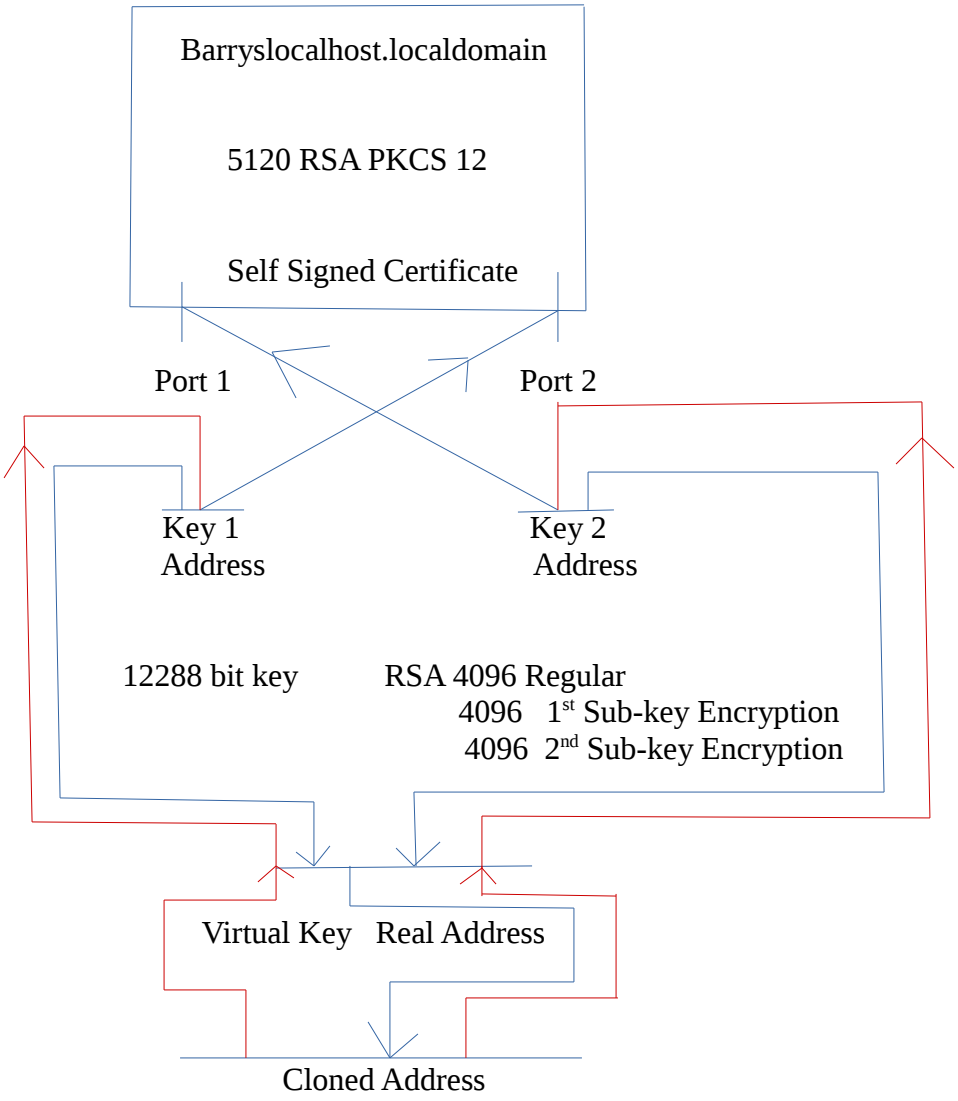
4). 48/ 24 = 2 Fields {+,-} X = Prime Number



Header Padded 48 Characters

View 3 Character Encoding UTF-64 Bits

4 Bytes = 1 Character



Method -1.3

12288 * 12288	=	150994944 Bits
150994944 / 64	=	2359296 Bits
2359296 / {64 bits * 4 Bytes} = 256	=	9216
√9216	=	96 Bits
96 / 4	=	24 Characters

Table of Character Fields

Barrys Scientific Based Products

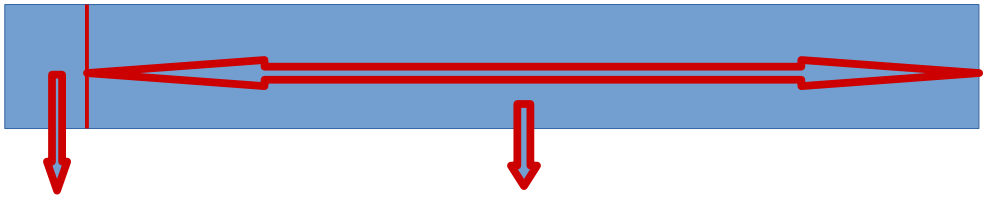
User Real Time Mode Choice

1). 24 / 2 = 12 Fields {+,-} X = Prime Number

2). 24 / 3 = 8 Fields {+,-} X = Prime Number

3). 24/ 4 = 6 Fields {+,-} X = Prime Number

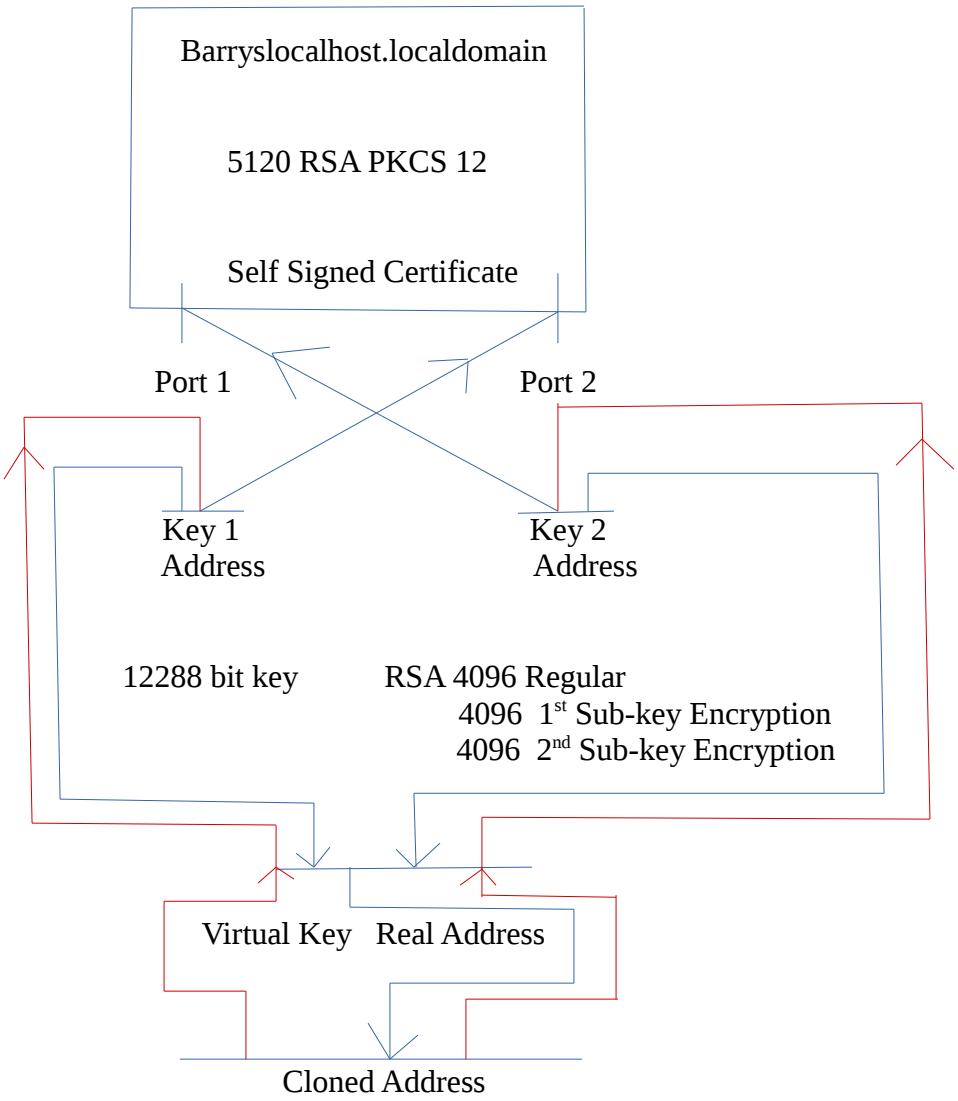
4). 24/ 6 = 4 Fields {+,-} X = Prime Number



Header Padded 24 Characters

View 4 Character Encoding UTF-128 Bits

4 Bytes = 1 Character



Method -1.4

12288 * 12288	=	150994944 Bits
150994944 / 128	=	1179648 Bits
1179648 / {128 bits * 4 Bytes} = 512	=	2304
√2304	=	48 Bits
48 / 4	=	12 Characters

Table of Character Fields

Barrys Scientific Based Products

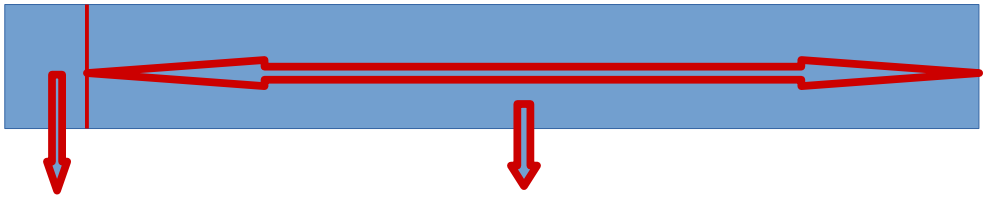
User Real Time Mode Choice

1). 12 / 2 = 6 Fields {+,-} X = Prime Number

2). 12 / 3 = 4 Fields {+,-} X = Prime Number

3). 12/ 4 = 3 Fields {+,-} X = Prime Number

4). 12/ 6 = 2 Fields {+,-} X = Prime Number



Header Padded 12 Characters

Chapter 2

A). Mathematical Formula and Process

B). Barry's Scientific Based Product Linear Based Key Exchange Process

Barry's Scientific Based Products Linear Key-UTF Mathematical Key Equation

Part A

Before the process is performed, The Mathematical Calculations must be initiated this is triggered by the following process.

1). Character Encodation is set to UTF 16, 32, 64,128

2). The Mathematical Equation is than performed as follows:
   a). X 2^{nd} power = 12288 * 12288 bits
   b). X 2^{nd} power / UTF View {16,32,64,128} = W
   c). W / UTF View { 16,32,64,128} * 4 = Y
   d). √ Y = Z
   e). Z / 4

3). User Interactive choice is than performed by the UTF View 16,32,64 and 128. Each UTF View, allots 4 fields and after the user choice is made the address field is than defined and calculates the nearest prime number set in a array. forcing the Data block two expand or contract depending on the nearest prime number example 12 fields are set and one more field is added via “padding” for a total of 13 fields another example is 6 fields are chosen I subtract 1 to get a prime number of 5 so I would remove the padded bits in the beginning of the IP Packet. this avoids duplication or copied keys on clipboards solving a IT Security issue of ASCII 8 bit code being easily identifiable.

The Equation is unique because it Expands and Contracts data within 1 process demonstrating the principal of Asymmetrical Energy namely the constant is 12288 bits the the variable is UTF Views using different Encodation schemes along with the User's Interactive choices creating a Dynamic Environment Non-predictable and demonstrates a better choice for Cyber Security Issues.

Barry's Scientific Based Product Linear Based Key Exchange Process

Part B

1). The Process is as follows

a). The certificate sends a Request from Key one or two to unlock the key from the Real address
b). The Real Address than sends a Request to the Virtual Key Cloned address.
c). The Real Address is copied to the Cloned Address and the field changes to the cloned address.
d). The new address from the Cloned address sends the address where it originated from either Key address one or two.
e). The Address Key one or two than send it's address to the Reverse port example Key one address sends to port two and Key two sends to port one address.

The process forces a Entanglement instead of calling from address one to port one it is entangled but with a new address that avoids copied addresses or duplication.

The process is also Unique in that it takes a Real Address and clones it with the address changing at the clone it than is entangled when sending the data block from the cloned address to the key and port address.

Chapter 3

Development of Project and Testing

I would like to provide technical information on the Development of this project.

1). 12288 Keys 4096 RSA and two sub key encryption created and published online.

2). Created PKCS12 RSA 5120 Linear Based placed in Certificate Store.

3). Set Encodation views through browser based software UTF 16 and 32.

4). tested cable ports plugging into a physical port and assigning it to a virtual port not plugged in.

If you like this Scientific work, Please come out and visit me on my website below

Barry Lee Crouse

Email barry@barrysscientificbasedproducts.com

Email crouseb395@gmail.com

website www.barrysscientificbasedproducts.com

02/27/2017