An Interactive Visualization Tool for the Interpretation of Mathematical Concepts behind Public Key Cryptography

Sikha O K,uchithra M ,Pinchu Prabha,Soman K P
Centre for excellence in Computational Engineering and Networking
Amrita School of Engineering
Coimbatore, India

ABSTRACT

Most of the engineering programs especially computer science have two or more security related subjects, but lack of active learning and practical experience in the classroom. Cryptographic algorithms which solve Security problems relay on specific mathematical areas such as modular arithmetic, probability and number theory. Unfortunately students feel difficulty to follow the concepts due to the underlying sophisticated mathematics; it is necessitating a fundamental change in our curriculum. Interactive pedagogical tools need to be introduced incrementally along with standard content in a way that makes the standard content easier to learn and vice versa. This work describes an interactive visualization tool which helps the student community to understand the mathematical concepts behind public cryptography algorithms using Microsoft Excel Spreadsheet. It is shown how the sophisticated maths can be visualized and implemented and also discussed some of the famous public key algorithms that the students at various level can do with the help of Microsoft Excel Spreadsheet.

General Terms

Security, Cryptography, Visualization tool

Keywords

Interactive tool, Maths behind public key cryptography, RSA visualization tool, ECC visualization tool

1. INTRODUCTION

Protection of secrets from theft has a history of at least 2000 years. Humans have developed several mechanisms to protect their data from an intruder [8]. Over time, all these activities have evolved and have become a vast area known as cryptography. During the ancient days, the predominant users of this art were government and military where it was considered as a tool to protect political secrets. At that time cryptography was only concerned with data confidentiality, changing the original data into an incomprehensible format such that only the indented user can understand the meaning [7]. As the computers and digital communication evolved during the early age of 90's, the field of cryptography has faced several challenges beyond privacy, which had been the main goal until that time [5]. Mathematical concepts behind the cryptographic algorithms are very tough to catch up, thus it has become one of the complex areas in the computer science field.

Traditionally, security related subjects follow chalk-talk instructional method in a passive class room atmosphere. This static learning procedure includes several copying stages: the teacher follow the notes from the preferred text book, then he copies those notes in to the black board, after that the students copies it in to their notebook. For the last few years, researchers are trying to incorporate the concept of computational thinking into the class room learning activities so that the students can improve their capabilities of using computational media to create, build, and invent solutions to new problems. A person is endowed with computational thinking if he/she can formulate and break down a problem at hand in such a way that major part of it is solvable by available computing tools [11]. If both the student and the instructor can actively participate in the classroom activities the learning rate can be improved [1][2]. Computational Thinking (CT) aims at creating sophisticated problem solvers instead of software users [11]. When students successfully combine the theoretical knowledge and computational methods they develop their identity as Computational Thinkers.

To the best of our knowledge, interactive pedagogical tools available for learning the complex mathematical theories behind cryptography is very less. Few papers 3][4][5][6] discussed the importance of interactive cryptography pedagogy. One of them [6] discuss the implementation of two symmetric algorithms DES and AES using Microsoft Excel Spreadsheet, while the other [5] explains the use of computer algebra tool such as Maple. The paper [3] discuss a visualization tool, DESvisual and [4] describes an interactive cryptographic learning tool.

Interactivity can be considered as a mutual action between the learner, learning material and learning system. For example reading an article by navigating through hypertext is a kind of interactivity [4]. Usage of graphical tools and textual effects which allow the user to differentiate the hypertext is highly recommended [7]. The main objective of this paper is to develop an interactive working environment for both teachers and undergraduate engineering students to train them to become proficient in security related subjects within a short period of time. Following sections describe the detailed implementation of mathematical concepts behind public key cryptography and RSA crypto system using Microsoft Excel Spread sheet.

2. MATHS BEHIND PUBLIC KEY CRYPTOGRAPHY AN OVERVIEW

Security offered by contemporary public key cryptosystems mainly relies on some number theoretic concepts and modular arithmetic that remain unbreakable. For example, RSA one of the famous cryptosystem works on modulo-n arithmetic, where n is the product of two prime large numbers. Modular arithmetic which is also referred to as clock arithmetic was proposed by Carl Friedrich Gauss in his book entitled Disquisitiones Arithmeticae at the end of 18th century. Modular arithmetic operations are analogous to 12-hour clock, where a day is divided in to 24 hours (2 twelve hours) for example let the time now is 9.00 then 4 hours later will be 1.00, we are performing modulo-12 addition. The interactive tool covered the following topics:

2.1 Prime Factorization

A prime number is any number greater than 1 and has no divisors other than 1 and itself. For example 3 is a prime number but 6 is not prime. Prime factorization is the process of finding which prime numbers multiply together to form the original number [6], the prime factorization of 6= 3*2.

2.2 Euclidian Algorithm

The Euclidean algorithm is one of the oldest known algorithms that appeared in Euclid's Elements (c. 300 BC). It is generally used for computing the gcd of two numbers by utilizing a simple iterative method.

THEOREM 1.

Input: A pair of integers (a,b)

Output: The greatest common divisor, gcd(a,b)

Assume that a>b (if not swap a and b). Apply the division algorithm iteratively. If the remainder is zero then gcd=b, else continue by dividing the consecutive divisors by corresponding remainders until the remainder becomes zero

2.3 Extended Euclidian Algorithm

Extended Euclidian algorithm can be considered as an extension of the Euclidean algorithm. In which addition to finding the greatest common divisor of two numbers this algorithm also evaluate integers x and y such that they should satisfy the Bezout identity [9].

$$ax+by=gcd(a,b)$$

The extended Euclidian algorithm is useful if the two numbers a,b are relatively prime to each other

2.4 Modular Inverse

In modular arithmetic the modular multiplicative inverse or mod inverse of an integer b (modulo n) is an integer b^{-1} such that $b * b^{-1} = 1 \mod n$.Modular inverse can be computed in two ways [9]

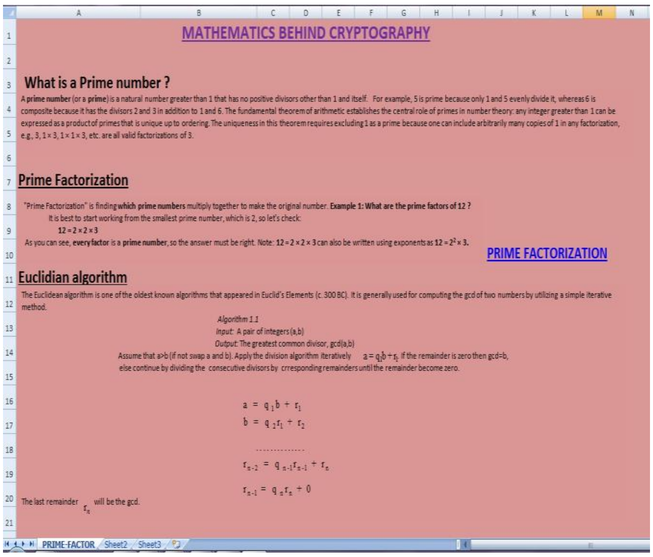
- rute-force or trial and error method
- sing Extended Euclidian algorithm

3. WHY EXCEL

This tool is developed using Microsoft Excel spread sheet. Excel is an excellent tool for the students to get practical learning experience from high school onwards. It is a computational platform that has the power to do any mathematical computation [9]. Students can work on Excel without any guidance as it is a user-friendly learning system [10]. The Excel can serve as such a valuable and versatile tool that helps the students to maximize the potential of their learning skills [9]. The present education system consists of merely delivering the concepts which in turn ruins the understanding ability of the students. It helps them to discover the hidden caliber

4. USER DOCUMENT

The entire tool has been coded in Visual Basic, the input data is read from the Microsoft excel spread sheet cells. User can enter the input in the cell; the VB code itself will access the data into the program. The following figure shows the home page of the interactive tool. This page gave the complete theoretical basics of the mathematical concepts explained in the above section. From this page the reader can navigate to different sections that will discuss later. By clicking on the hyperlink PRIME FACTORIZATION it will open a new window as shown in the figure 2. Enter the number on the specified field and click on the COMPUTE PRIME FACTOR button. It will print the factors. In the Euclidian algorithm window, there are two text fields to enter the two numbers whose greatest common divisor is going to compute. Click on the activation button named COMPUTE EUCLIDIAN [GCD] to execute the algorithm and the result will appear in the text field. Figure 3 shows windows corresponding to modular inverse and extended Euclidian algorithm modules. Enter the two numbers in the corresponding text fields, and click the COMPUTE EXTENDED EUCLIDIAN button. The system will print the results. The modular inverse module is designed to show how to evaluate the modular inverse of a given number using extended Euclidian algorithm. This tool also includes ISBN number checker and credit card checker, which will enable the student to understand how online banking is done by keeping the secret information concealed. The corresponding modules are shown in the Figure 4.



MATHEMATICS BEHIND CRYPTOGRAPHY

What is a Prime number ?

A prime number (or a **prime**) is a natural number greater than 1 that has no positive divisors other than 1 and itself. For example, 5 is prime because only 1 and 5 evenly divide it, whereas 6 is composite because it has the divisors 2 and 3 in addition to 1 and 6. The fundamental theorem of arithmetic establishes the central role of primes in number theory: any integer greater than 1 can be expressed as a product of primes that is unique up to ordering. The uniqueness in this theorem requires excluding 1 as a prime because one can include arbitrarily many copies of 1 in any factorization, e.g., 3, 1 × 3, 1 × 1 × 3, etc. are all valid factorizations of 3.

Prime Factorization

"Prime Factorization" is finding **which prime numbers** multiply together to make the original number. **Example 1: What are the prime factors of 12 ?**

It is best to start working from the smallest prime number, which is 2, so let's check:

12 = 2 × 2 × 3

As you can see, **every factor** is a **prime number**, so the answer must be right. Note: **12 = 2 × 2 × 3** can also be written using exponents as **12 = 2^2 × 3.**

PRIME FACTORIZATION

Euclidian algorithm

The Euclidean algorithm is one of the oldest known algorithms that appeared in Euclid's Elements (c. 300 BC). It is generally used for computing the gcd of two numbers by utilizing a simple iterative method.

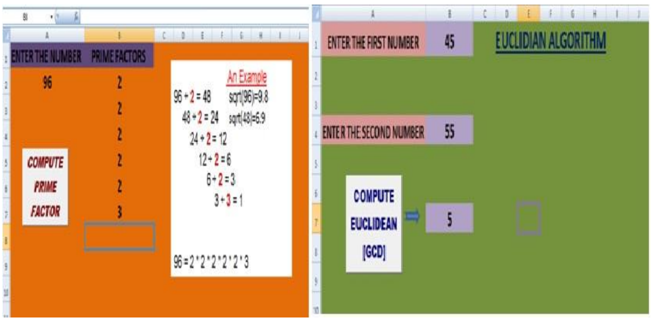
Algorithm 1.1
Input: A pair of integers (a,b)
Output: The greatest common divisor, gcd(a,b)

Assume that a>b (if not swap a and b). Apply the division algorithm iteratively $a = q_1b + r_1$ If the remainder is zero then gcd=b, else continue by dividing the consecutive divisors by crresponding remainders until the remainder become zero.

$$a = q_1b + r_1$$
$$b = q_2r_1 + r_2$$
$$\cdots\cdots\cdots$$
$$r_{n-2} = q_{n-1}r_{n-1} + r_n$$
$$r_{n-1} = q_nr_n + 0$$

The last remainder r_n will be the gcd.

Fig 1: Home page of the tool

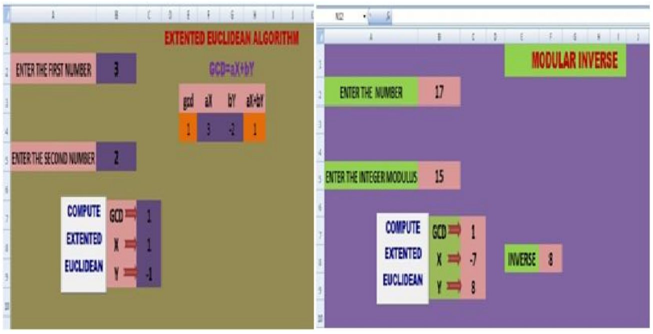


ENTER THE NUMBER: 96
PRIME FACTORS: 2, 2, 2, 2, 2, 3

An Example
96÷2=48 sqrt(96)=9.8
48÷2=24 sqrt(48)=6.9
24÷2=12
12÷2=6
6÷2=3
3÷3=1
96=2*2*2*2*2*3

EUCLIDIAN ALGORITHM
ENTER THE FIRST NUMBER: 45
ENTER THE SECOND NUMBER: 55
5

Fig 2: Euclidian and prime factorization window



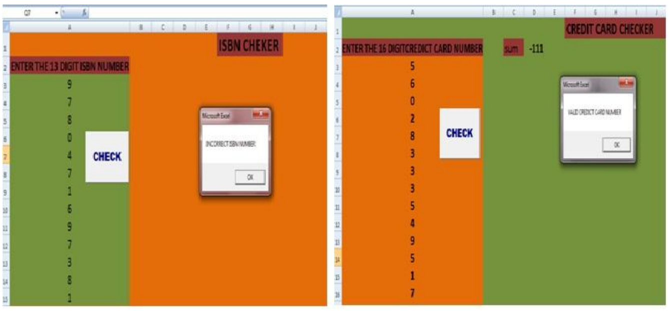
EXTENTED EUCLIDEAN ALGORITHM
GCD=aX+bY
ENTER THE FIRST NUMBER: 3
ENTER THE SECOND NUMBER: 2

gcd	aX	bY	aX+bY
1	3	-2	1

GCD 1
X 1
Y -1

MODULAR INVERSE
ENTER THE NUMBER: 17
ENTER THE INTEGER MODULUS: 15
GCD 1
X -7
Y 8
INVERSE 8

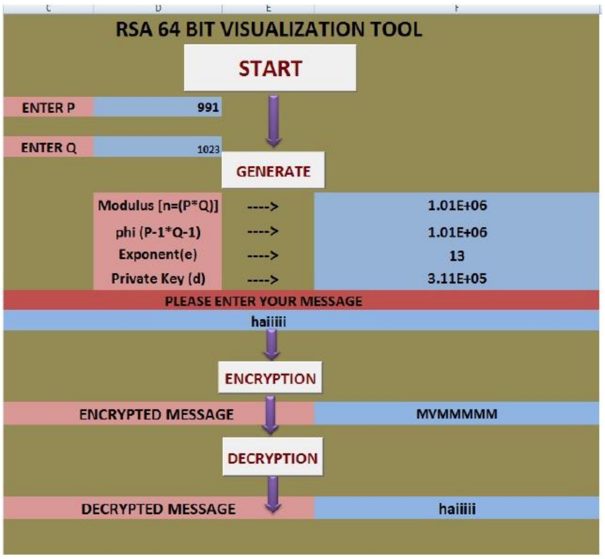
Fig 3: Extended Euclidian and modular inverse window



ISBN CHEKER
ENTER THE 13 DIGIT ISBN NUMBER: 9 7 8 0 4 7 1 6 9 7 3 8 1
Microsoft Excel: INCORRECT ISBN NUMBER

CREDIT CARD CHECKER
ENTER THE 16 DIGITCREDIT CARD NUMBER: 5 6 0 2 8 3 3 3 5 4 9 5 1 7
sum -111
Microsoft Excel: VALID CREDIT CARD NUMBER

Fig 4: ISBN and CREDIT CARD checker window



RSA 64 BIT VISUALIZATION TOOL
ENTER P: 991
ENTER Q: 1023
Modulus [n=(P*Q)] ----> 1.01E+06
phi (P-1*Q-1) ----> 1.01E+06
Exponent(e) ----> 13
Private Key (d) ----> 3.11E+05
PLEASE ENTER YOUR MESSAGE: haiiiii
ENCRYPTED MESSAGE: MVMMMMM
DECRYPTED MESSAGE: haiiiii

Fig 5: RSA visualization tool

5. IMPLEMENTATION

The entire tool has been developed using Excel-VBA coding. User can directly access the VBA user interface from the excel sheet by clicking Alt+F11 keys on the key board, it will displays the VBA coding window where we can start writing program. VBA instructions are very simple and similar to basic C language; hence an undergraduate student can easily handle the coding section. There are commands to read an input from the Excel cells into the VBA user interface also for printing output in to the Excel cells. n = Cells (1, ”A”).Value command will read the value inserted in the cell A1 in to the VBA variable n. Similarly the command Cells (1, ”B”). Value = n will copy the value of n back to the cell B1. The following section explains the VBA algorithm for developing each module in the interactive tool.

5.1 Algorithm

1) Prime factor

Initialize an output array flist() as Variant.

1. Read the number to be factorized from the excel sheet in to the VBA variable say n by specifying the cell address.
2. Initialized the variable fac as 2
3. While fac<sqrt(n) do the following steps. [To import the worksheet function sqrt on to the VBA working environment use the command “Application.WorksheetFunction.function name”
   - If n mod fac=0 then store the value of fac into the output array

     n=n/fac
   - Else increment fac
   - End if
   - End while
4. Copy the values in the output array flist(), in to the excel sheet using the command “Cells(i, "b"). Value = flist(i)” and increment “i”.

2) Euclidean algorithm

1. Read the two numbers whose GCD has to be find in to the VBA variables a,b respectively.

```
2. Find the maximum of a,b using the worksheet function max(a,b) and store the result in the variable Max.
3. Similarly, find the minimum of a,b using the worksheet function min(a,b) and store the result in the variable Min.
4. q=Max/Min. Round the result q in to single precision using the function floor(q,1) since excel support precision of 5 to 6 decimals.
5. r=Max-q*min
6. While r>0 do the following steps
       • Max=Min
       • Min=r
       • Repeat the steps 4 and 5
7. End while
8. Copy the value of Min in to the excel sheet which will be the GCD(a,b).
```

3) Extended Euclidian algorithm

```
1. Read the input numbers from excel sheet to the variables a,b
2. Find maximum and minimum as shown in the previous algorithm and store it in Max & Min respectively.
3. Initialize two variant arrays U(3) and V(3) and store the values
       U (1) =Max, U (2) =1, U (3) =0
       V (1) =Min, V (2) =0, V (3) =1
4. While V(1)>0 do the following steps
   • For each values of U and V evaluate
               W=U-Floor (U (1)/V (1)) * V
               U=V
               V=W
5. End while
6. Gcd=U (1), and copy the value of Gcd into the excel sheet.
```

4) Modular inverse

```
1. Follow the entire steps of Extended Euclidian algorithm.
2. If Max=a then x=U(2) else x=U(3)
3. Inverse=x mod b, copy the result in to the excel sheet.
```

5) ISBN checker

```
1. Read the 13 digit ISBN number into the variant array isbn(13).
2. Initialize the variant array v(13) as 1, and made the alternative values of the array as 3.
3. For each values of isbn (13) do the following computation
       • check=10-v(i)*isbn(i) mod 10
       • Increment i up to 12
4. If check=isbn(13), display the message that the entered number is correct else the number is wrong.
```

6) Credit card checker

```
1. Read the 16 digit Credit card number into the variant array credit (16).
2. Initialize the variant array v(16) as 1, and made the odd instances of the array as 2.
3. For each values of credit (116) do the following computation
       • P(i)=v(i)*credit(i) mod 10
   • Increment i up to 15
   • Find the sum of each element of the array P, and change the sign and store it in check
4. If check=credit(16), display the message that the entered number is correct else the number is wrong.
```

6. CONCLUSION

There is a widespread need for high-quality system security professionals who is having the ability to learn the concepts within a short period of time. Colleges can help to meet this requirement by modernizing the existing information security courses. By introducing active learning with rapidly changing technologies teachers can help the students to remove their learning difficulties. To meet the demand for hands-on classroom activities while learning mathematics behind security related subjects we have developed an interactive tool using Microsoft Excel Spreadsheet. This active learning tool will help the students to understand the complicated mathematical concepts easily and quickly.

7. REFERENCES

[1] Information Security Course Based on Applications of Management Techniques in Digital Systems for Business Colleges, Herath et al, The 2002 International Conference on Security and Management, (SAM02), Las Vegas, USA, 23-25, June 2002

[2] Integration of computer security laboratories into computer architecture courses to enhance undergraduate curriculum, Herath et al., Proceedings of Workshop on Computer Architecture Education, June 9-11, 2003, San Diego, CA

[3] DESvisual: A Visualization Tool for the DES Cipher,Jun Tao, Jun Ma, Melissa Keranen,Jean Mayo, Ching-Kuang Shene, march 26,2011

[4] Learning the Related Mathematics to Cryptography by Interactive Way, Mohamed Salim Trigui , Daniyal M. Alghazzawi, MECS , March 2012

[5] Alasdair McAndrew. Teaching Cryptography with Open-Source Software. In ACM 39th SIGCSE Technical Symposium, pages 325329, 2008.

[6] Oi-Shong Chok and Susantha Herath. Computer SecurityLearning Laboratory: Implementation of DES and AES Algorithms using Spreadsheets. In MICS 2004 Proceedings,April 2004.

[7] C. E. Iglesias, et al., ”Calculus b-learning with java tools,”WSEAS Transactions on ADVANCES in ENGINEERING EDUCATION, pp. 295-305

[8] G. H. Hardy, Prime numbers, British Association Report,Britist Association, Manchester, 1915, (In Collected Papers”,vol. 2), pp. 350-354.

[9] Computation Of Continuous Wavelet Transform Using Microsoft Excel SpreadSheet Pinchu Prabha, Sikha O K, Suchithra M, Sukanya P, Sowmya V, K P Soman

[10] Visualization of OFDM using Microsoft Excel Spreadsheet in Linear Algebra Perspective,Anand R, Pinchu Prabha, Sikha O.K, Suchithra M, Sukanya P, Sowmya V, Soman K.P