Engaging Students in Learning Public Key Cryptography

Vamsi Gondi, David Hua and Biju Bajracharya

Ball State University

vkgondi@bsu.edu; dhua@bsu.edu; bajracharya@bsu.edu

Abstract
One major issue when teaching students about security is the complexity of the mathematics used in encryption. Public Key Cryptography (PKC) is one such concept where students need to use high-level mathematical skills. Through previous interactions in the classroom, the traditional chalk and board approach to teaching PKC was not effective in the retention of the concepts in the long run. To improve the retention level, two pedagogical techniques were developed that involved students working in pairs and accomplishing security tasks. The impact was measured with student feedback forms and with the reference to Blooms taxonomy.

Introduction

Public key cryptography is used for message authentication and key distribution in modern computer communications (Mathivanan, Sharmathi, & Akshaya, 2015). It is truly an advanced encryption technique applied across security domains. Public key cryptography uses algorithms that are made up of mathematical functions rather than employing changing bit patterns and superimposition (Barker, 2016). To comprehend these algorithms, students need high level mathematical computation skills. Studies suggest that most students lack these capabilities (ECPI University, n.d.; Thompson, 2019). There is a need to find alternative pedagogical techniques to make students understand the inner functioning of public key cryptography.

Two cryptographic techniques; RSA public-key encryption algorithm (Ireland, 2019) and Diffie-Hellman algorithm (Rescorla, 1999) were introduced as a part of the computer security course. We used alternative pedagogical techniques for delivering this content. We assessed the impact of the course through blooms taxonomy levels (Armstrong, 2010) and through student's feedback forms.

The paper is organized as follows, we introduce RSA and pedagogical techniques to teach RSA algorithm. We introduce Diffie-Hellman algorithm and the pedagogical techniques that were used to teach Diffie-Hellman algorithm. Blooms taxonomy impact and student feedback is described in this paper.

Public Key Cryptography

Public key cryptography uses two separate keys; public key and private key to encrypt and decrypt data. The public key of the user is distributed to others and the private key is kept with the owner. The users generally exchange keys through public certificate authorities such as Verisign.

For instance, Alice and Bob want to communicate with each other, both Alice and Bob generate public keys and private keys and exchange their public keys. If Alice want to communicate with Bob, Alice uses Bob's public keys to encrypt data and Bob uses its private key to decrypt data. Alice also can use its own private key to encrypt data, and Bobs uses Alice public key to decrypt the data.

RSA algorithm

RSA was developed in 1977, it uses public key {e, n} to convert plaintext block M into ciphertext block C, and private key {d, n} to convert ciphertext block to plaintext block.

$$C = M^e \bmod n$$
$$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$$

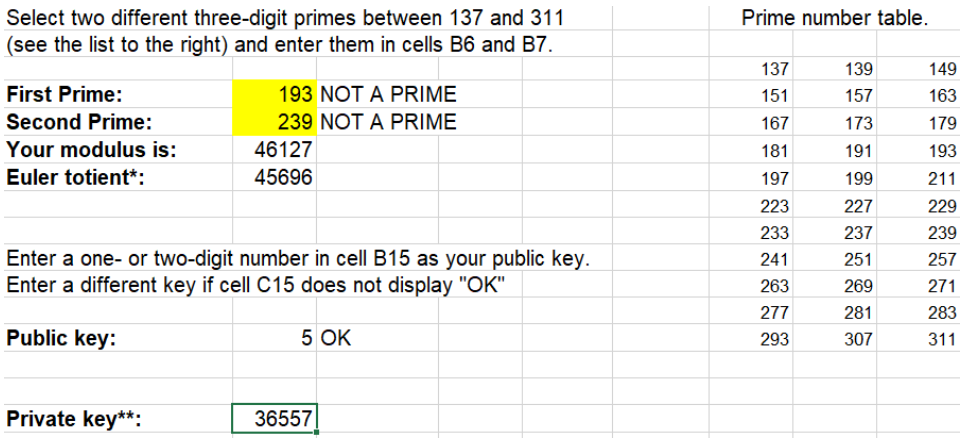
RSA algorithm involves multiple steps to encrypt and decrypt data.

Step 1. Select two prime numbers p and q
Step 2. Calculate modulus, $n = p * q$
Step 3. Calculate Euler totient, $\emptyset(n) = (p-1) * (q-1)$
Step 4. Select e, such that, $\gcd(\emptyset(n), e) = 1; 1 < e < \emptyset(n)$
Step 5. Calculating d, $de \bmod \varphi(n) = 1$
Step 6. Public key, $KU = \{e, n\}$
Step 7. Private key, $KR = \{d, n\}$
Step 8. Encrypting plaintext M to ciphertext C, $C = M^e \bmod n$
Step 9. To decrypt ciphertext C, $M = C^d \bmod n$

Pedagogical techniques used to teach RSA

As shown in the previous section there are multiple steps and complicated math involved to teach RSA. During our previous sessions, we used the selection of p and q values and used to solve the math, it was challenging making students comprehend all the steps and making them understand the math behind it. To overcome this, we used Excel sheets asks students to select values and perform RSA for themselves and we assisted them on how to calculate GCD (greatest common divisor), modulo, etc.

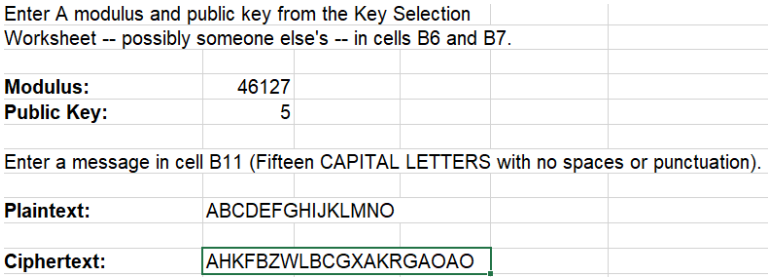
In the classroom session we asked students to be in two pair groups, both performing encryption and decryption, they were provided with an excel sheet. In the initial step, the students asked to select two prime numbers (p and q) from the list provided, the formulas inside Excel calculates the modulus and Euler totient as show in figure 1. Then they were asked to select a prime integer and enter in cell B15 and change to new integer until cell C15 displays OK. In this step, we explained how GCD is calculated with the selected integer. Once the public key is selected, the system calculates the private key.



Select two different three-digit primes between 137 and 311 (see the list to the right) and enter them in cells B6 and B7.			Prime number table.		
			137	139	149
First Prime:	193	NOT A PRIME	151	157	163
Second Prime:	239	NOT A PRIME	167	173	179
Your modulus is:	46127		181	191	193
Euler totient*:	45696		197	199	211
			223	227	229
			233	237	239
Enter a one- or two-digit number in cell B15 as your public key.			241	251	257
Enter a different key if cell C15 does not display "OK"			263	269	271
			277	281	283
Public key:	5	OK	293	307	311
Private key:**	36557				

Figure 1

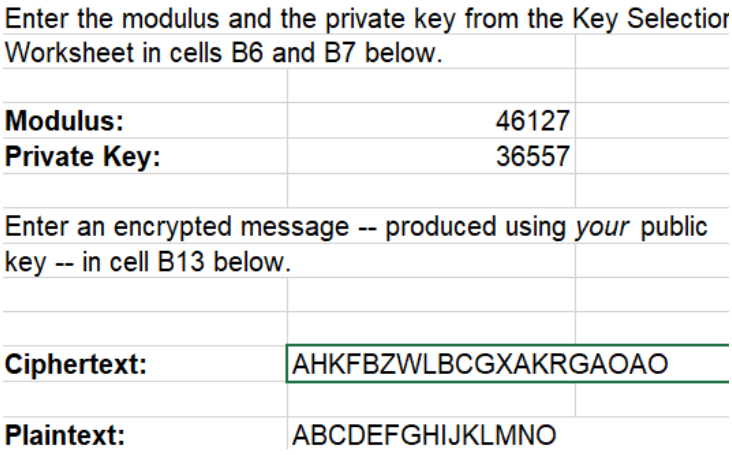
For encrypting plain data, the students need to use their lab partner's public key, they exchange their public keys with each other. In the encrypting Excel sheet, they entered the partner's public key and plaintext to be encrypted as shown in figure 2. The excel sheet generates the ciphertext as shown in figure 2. Then students write their ciphered text on a notepad and exchange with their partners.



Enter A modulus and public key from the Key Selection Worksheet -- possibly someone else's -- in cells B6 and B7.	
Modulus:	46127
Public Key:	5
Enter a message in cell B11 (Fifteen CAPITAL LETTERS with no spaces or punctuation).	
Plaintext:	ABCDEFGHIJKLMNO
Ciphertext:	AHKFBZWLBCGXAKRGAOAO

Figure 2

For decrypting, students use their private key and ciphertext exchanged from their partners, they enter the details in the excel sheet as shown in figure 3, once the step is completed plaintext is revealed.



Enter the modulus and the private key from the Key Selection Worksheet in cells B6 and B7 below.	
Modulus:	46127
Private Key:	36557
Enter an encrypted message -- produced using *your* public key -- in cell B13 below.	
Ciphertext:	AHKFBZWLBCGXAKRGAOAO
Plaintext:	ABCDEFGHIJKLMNO

Figure 3

Diffie-Hellman Algorithm

The Diffe-Hellman algorithm is used for exchanging secret keys between two users that can be used for encryption and decryption. The students need prior knowledge of primitive root modulo. The algorithm uses steps shown below for users A and B.

Step 1. A prime number q and an integer α that is a primitive root of q is selected by users A and B
Step 2. User A select random integer X_A, and calculates Y_A, $Y_A = \alpha^{X_A} \bmod q$.
Step 3. User B select random integer X_B, and calculates Y_B, $Y_B = \alpha^{X_B} \bmod q$.
Step 4. User A exchange its Y_A value with user B, User B exchange its Y_B value with user A
Step 5. User A calculates key K, $K = (Y_B)^{X_A} \bmod q$
Step 6. User B calculates key K, $K = (Y_A)^{X_B} \bmod q$

Diffie-Hellman algorithm in-class activity

As discussed earlier, it was challenging for students to comprehend the algorithm and math involved with the traditional instruction techniques. To overcome the issue, we developed a pedagogical technique involving students creating keys for themselves. We provided an online tool where students can perform power mod calculations (Mount Holyoke, 2003) and notes on a small sheet of paper as shown in Table 1. The students are divided into pairs of two, they were provided with prime number q and α values and explained the math how those values were chosen using the primitive root mod. Students are also provided with X values, with all these three integer values and formula involved in step 2 and 3 students calculate Y values using power mod calculator. The students exchange the Y values on the piece of paper to their partners. With the available Y values from their partners, they calculate the key mentioned in step 5 and 6. The complete key calculations are shown in Table 2

Team 1 - Alice	**Team 1 – Bob**
α = 3	α = 3
q = 7	q = 7
X_A = 5	X_B = 11
Calculate Y_A =	Calculate Y_B =
Y_B = (from Bob)	Y_A = (from Alice)
Calculate K =	Calculate K =

Table 1

Team 1 - Alice	**Team 1 – Bob**

$\alpha = 3$	$\alpha = 3$
q = 7	q = 7
$X_A = 5$	$X_B = 11$
Calculate $Y_A = 5$	Calculate $Y_B = 5$
$Y_B = 5$ (from Bob)	$Y_A = 5$ (from Alice)
Calculate K = 3	Calculate K = 3

Table 2

Impact measurement – Blooms Taxonomy

It is crucial to measure the teaching outcomes based on a scale to ensure there is learning in the classroom session. We chose Bloom's Taxonomy, which is a widely used assessment technique used for identifying the outcome. Bloom's Taxonomy measures outcomes such as remembering, understanding, applying, analyzing, evaluating and creating. Remembering being the lowest and creating is the highest level. In traditional teaching techniques used in teaching both the algorithm's attained only two levels: Understanding and remembering. With the proposed pedagogical techniques students were able to apply the concepts; analyze and evaluate the concepts in terms of why and how they chose particular numbers instead of random numbers; and how to calculate using these specific math content. In the end the students were able to create keys, encrypt data and decrypt cipher text using the tools provided in the class.

Student Feedback

At the conclusion of the session, twenty-five students completed a feedback survey. One area of concern was whether students would understand the purpose of the session. All but one student indicated that the learning objectives were clearly conveyed. After using the presented teaching strategies, 100% of the students indicated that they session was effective in understanding the Diffie-Hellman algorithm used in the PKC process. The handouts were helpful to 92% of the students in understanding the cryptographic concepts. The only minor issue indicated in the survey was that three of the students did not recognize the importance of the Diffie-Hellman algorithm and PKC.

Conclusion

Computer science, especially computer security, network security and cybersecurity areas need high mathematical skills. Most of the top universities have special math courses which are mandatory for enrolling in computer science programs. As an alternative, we proposed new pedagogical techniques which are helpful for the students for the retention of the concepts in the classroom sessions. The proposed PKI pedagogical techniques were effective in teaching a complex concept. We also assessed effectiveness of the techniques used in the classroom session with respective to blooms taxonomy levels. Also, student feedback was very encouraging on how they personally involved in the learning process.

References

Armstrong, P. (2010, June 10). Bloom's Taxonomy. Retrieved August 15, 2019, from Vanderbilt University website: https://wp0.vanderbilt.edu/cft/guides-sub-pages/blooms-taxonomy/

Barker, E. (2016). *Recommendation for Key Management, Part 1: General* (No. NIST Special Publication (SP) 800-57 Part 1 Rev. 4). https://doi.org/10.6028/NIST.SP.800-57pt1r4

ECPI University. (n.d.). How is Math used in Cyber Security? Retrieved August 15, 2019, from https://www.ecpi.edu/blog/how-s-math-used-in-cyber-security

Ireland, D. (2019, June 9). RSA Algorithm. Retrieved August 15, 2019, from RSA Algorithm website: https://www.di-mgt.com.au/rsa_alg.html

Mathivanan, K., Sharmathi, R., & Akshaya, R. (2015). Overview of Modern Cryptography. *International Journal of Computer Science and Information Technologies*, *6*(1), 2015, 350–353.

Mount Holyoke. (2003). PowerMod Calculator. Retrieved August 15, 2019, from https://www.mtholyoke.edu/courses/quenell/s2003/ma139/js/powermod.html

Rescorla, E. (1999, June). Diffie-Hellman Key Agreement Method. Retrieved September 24, 2019, from https://tools.ietf.org/html/rfc2631

Thompson, V. (2019). The Need for Basic Math & Science Skills in College Students. Retrieved August 15, 2019, from Sciencing website: https://sciencing.com/the-need-for-basic-math-science-skills-in-college-students-12751440.html