Teaching Tip

An Inexpensive Device for Teaching Public Key Encryption

Norman Pendegraft
College of Business and Economics
University of Idaho
Moscow ID 83844-3161
norman@uidaho.edu

ABSTRACT

An inexpensive device to assist in teaching the main ideas of Public Key encryption and its use in class to illustrate the operation of public key encryption is described. It illustrates that there are two keys, and is particularly useful for illustrating that privacy is achieved by using the public key. Initial data from in class use seem to confirm its utility.

Keywords: Public Key Encryption

1. INTRODUCTION

Information Assurance (IA), the general problem of maintaining information system security, is an important topic for Information Systems (IS) majors as well as for general business students. While there is a considerable student interest, the topic is highly technical, and so it presents problems when teaching a non technical audience. One specific IA issue of great economic importance is public key encryption infrastructure (PKI). Students seem to be very interested, but they struggle with remembering that the public key is used for guaranteeing privacy. This paper describes a device used to illustrate the operation of PKI.

Temkin (2007) confirms the importance of teaching encryption basics to general students. Yurcik and Doss (2001) discuss several approaches to teaching IS security. Although their focus seems to be on a course devoted entirely to security, their conclusions seem valid for a more general audience. They identify topic selection as the most difficult problem. They also note that differences in learning styles are important. In particular, many students respond best to a hands-on approach. They also recommend real life cases. They discuss a number of approaches in more detail including projects, research, and labs. Several other authors describe a variety of approaches for teaching about security including using a chat room (Mitchener and Vahdat, 2001) and a laboratory exercise (Rawles and Baker, 2003) Sanders (2003) describes a project involving identifying a hacker. Cao et.al. (2002) used a programming project in which students develop applications that exchange encrypted traffic. Reid, Platt, and Wei (2005) also describe a teaching module to introduce encryption. Many of these are appropriate for a IS course with a technical audience and substantial time to devote to security, but they appear to be less attractive for a short presentation to a general audience.

Because of its importance in e-commerce, PKI is one of the most important topics for general business audiences. (It is also fun.) Teaching encryption is challenging because understanding modern ciphers requires a high level of mathematical sophistication. The challenge is making the structure of PKI accessible to a more general audience.

This device described here was developed for the IS component of our Integrated Business Curriculum, a 17 credit two semester course covering all of the business core topics (Pendegraft et.al. 2000). In that course we have a general audience and generally spend 3-4 hours on IA of which only part is devoted to encryption. It has been the author's experience, that after a lecture and discussion, many still fail to grasp the key idea, namely that the receiver's public key is used to ensure privacy. Instead, their intuition tells them that a private key should be used for privacy.

A search of the internet revealed only one other device to help teach encryption (Yuan, 2008), but it is expensive. Further, its operation is unclear from the web site. It appears to be a lockable box with two different keys, one for locking and the other for unlocking. It is not clear how well it enhances student's understanding. A patent search revealed no similar devices.

The device described herein is intended to illustrate PKI in concrete terms, and at low cost. Further, the device is simple enough that the students can understand how it works, thereby increasing the likelihood that they will remember the lesson. The author has used it to teach the topic and found that students responded well to the demonstration.

The remainder of the paper briefly describes PKI, describes the device and its use in the classroom, and offers some evidence suggesting that the device was well received.

2. PUBLIC KEY INFRASTRUCTURE

Public key encryption is described by many authors. For example, Fitzgerald and Dennis (2009) offer a nice, elementary discussion while Stallings (2006) presents a more detailed mathematical discussion. The theory of PKI is beyond the scope the course in which this discussion takes place. Consequently, only a brief outline of the operation of PKI (of similar scope to the classroom discussion) will be given here. The device illustrates only how PKI behaves so far as users are concerned, but not the mathematics behind the algorithms.

PKI uses asymmetric encryption which means that there are two keys. One key is used for encryption and another that is used for decryption. Thus, each user has a pair of keys. The keys are chosen so that if one is used to encrypt a message the other must be used to decrypt and vice versa. They are chosen in such a way that even if an attacker knows one of them, finding the other is computationally intractable. One (the public key) is posted in a public place. The other (the private key) is secret and is known only to its owner.

To send a private message the sender (S) encrypts a message using the public key of the receiver (R). The receiver decrypts the received, encrypted message with her own private key. Since this private key is the only one that works, secrecy is ensured. This process is illustrated in Figure 1.

To create a digital signature, the sender (S) creates a digest of the message. The digest is encrypted with her private key. Both the message (in the clear) and the encrypted digest are sent to the receiver (R) who decrypts the digest with the sender's public key. The digest is compared to the message and if they match, this ensures the identity of the sender since only the owner of the private key could have created the message digest. This is illustrated in Figure 2. Privacy can also be ensured by using the recipient's public key to encrypt both the message and digital signature.

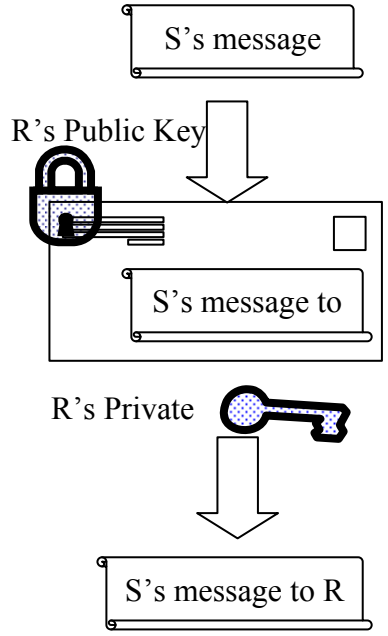

Figure 1. Privacy in PKI

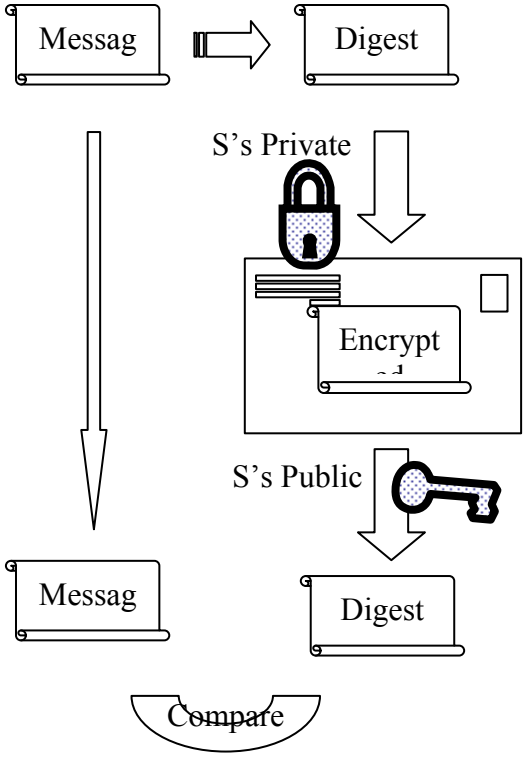

Figure 2. Digital Signature

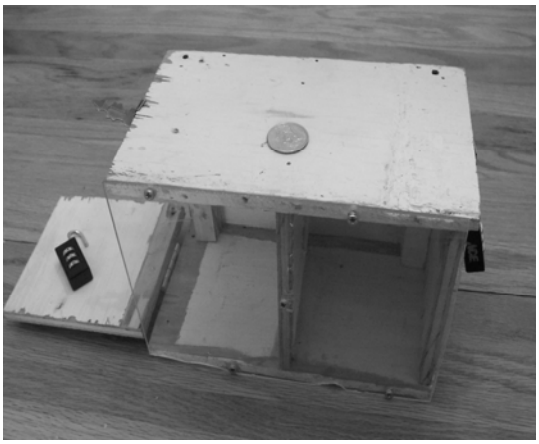

Figure 3. The Box

3. THE DEVICE

3.1 Description

The device is a simple box with 2 doors in opposite ends. As can be seen from the photograph in Figure 3, each door is secured by an inexpensive combination luggage lock. The box is divided internally by a wall with a "mail slot" opening (a 1" hole in the prototype). A cup hook is inserted somewhere on the private side to allow for demonstration of digital signature. This feature is described later. The quarter on the box illustrates its size.

One door is designated "private" and the combination of that lock is revealed only to the owner of the box. The other door is designated "public" and the combination of that lock is written on the blackboard. One of the side walls is made of clear plastic, literally making the operation of the box transparent. This helps the students by clarifying how the box works.

3.2 Class Use

Figure 4 illustrates sending a secured message. The instructor announces his public key by writing it on the board. The sender (a student) writes a message to the instructor on a sheet of paper. The sender then unlocks and opens the "public" door and pushes the message through the slot. The public door is then locked. The box is passed around the room and students are invited to "intercept the message". Of course, they cannot. Finally, the box is delivered to the instructor who opens the private door using the private key and reads the message. Figure 5 shows a photo of the box being loaded with a secret message.

Illustrating a digital signature requires using the cup hook referred to above. The sender (the instructor) writes two copies of the message. One (the message) is taped message-side-up on the outside of the box. The second (the digest) is placed in a plastic bag. The sender opens the private door, and pushes the message and part of the bag through the slot to the public side. The "tail" of the bag is affixed to the cup hook on the private side as illustrated in Figure 6. The private door is then locked. The box is again passed around the room to a student recipient. Note that every one can read the message. The recipient opens the public side of the box and retrieves the message digest by cutting open the bag. The recipient is confident that the message could only have been placed there by the person with the private key, i.e. the instructor. Figure 7 shows a photo of the box with a signed message. Since running it in class, it has occurred to us that it is not necessary to cut the bag if the message digest can be read through it. We will try that next time.

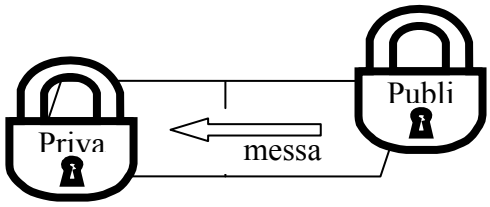

Figure 4. Illustrating Privacy

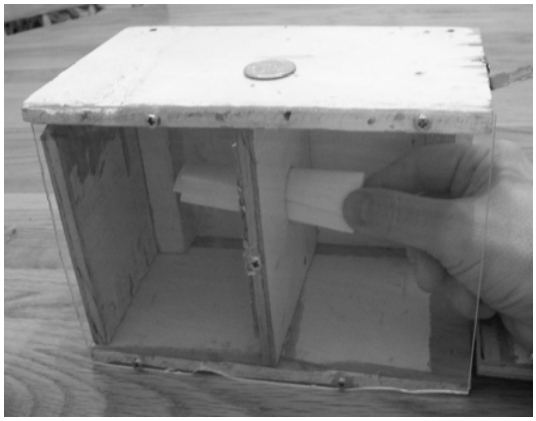

Figure 5. Inserting a Message

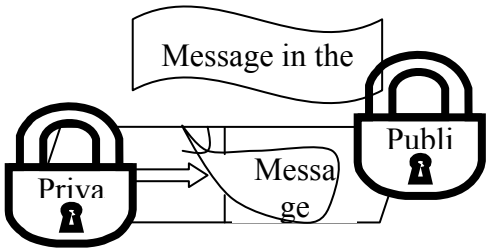

Figure 6. Digital Signature

Figure 7. A "Signed" Message

To illustrate the importance and difficulty of key management, the instructor may write the following announcement on the blackboard: "Alice's public key is 123". Someone else may then write elsewhere on the board: "Alice's public key is 456". This issue before the class now is which one to believe. This nicely leads to a discussion of key management and certificates.

4. INITIAL FINDINGS

We used the device in a lecture, and to gauge its value, we gave a short, anonymous, non credit quiz and questionnaire (see Appendix) after the lecture. We received 30 complete and 5 partial answers out of a class of about 45. The responses are summarized in Table 1, and while not as good as we would like, they seem better than would be expected after a normal one hour lecture. Certainly, the attitude toward the use of the device was positive (Table 2) with 30/35 (86%) agreeing or strongly agreeing (an only 1 disagreeing) that this tool and other demonstration tools were useful. Interestingly, the most common error was in selecting the SENDER's key for privacy. As noted above, this is the difficult idea, and even with the tool, it proved difficult.

The quality of the data is limited by the fact that the quiz was optional and non credit and there was no control

group. There may also be some reporting bias in that the five partial responses were entirely incorrect. It seems reasonable to assume that those who did not respond might also have done poorly. This lecture was before we came up with the idea of displaying the message in the open for a digital signature, so the data does not reflect the improvements suggested here. Nevertheless, the quiz results suggest to us that the device was useful. Certainly, the survey results suggest that the students thought so.

Score (out of 4 points)	0	1	2	3	4
Frequency	0	1	4	9	16

Table 1. Quiz Results

	SA	A	N	D	AD
I find demonstration tools like the message box useful	**15**	**15**	**5**	**0**	**0**
The message box will help me remember how public key encryption works	**11**	**19**	**4**	**1**	**0**

SA=Strongly Agree; A=Agree; N=Neutral; D=Disagree; SD=Strongly Disagree

Table 2. Survey Results

5. CONCLUSION

As noted we will continue to experiment with the use of the bag in illustrating a digital signature. The author plans to build a second, larger box. The second box, if large enough to accept the smaller box as a message would make it possible to illustrate a private and signed message. The second box could also be used as a certificate authority (CA) to illustrate the use of the CA's public key to retrieve a trusted public key for the recipient.

PKI is an important topic in understanding electronic commerce, but it is difficult to learn. In particular, it is difficult for students to remember that the receiver's public key is used to insure privacy. This device makes it possible to illustrate that idea in a concrete way. Students responded favorably to the device, and it seems to help them understand the basics of public key encryption and remember the idea.

6. ACKNOWLEDGEMENTS

The author thanks an anonymous referee for several very helpful suggestions. He also thank his colleagues Bob Stone and Mark Rounds for helping with the in class sessions.

7. REFERENCES

Cao, Q., David, J.,Bai, X., & Katter, O. (2002), "Using ASP-Based Message Encryption Project To Teach Information Security Concepts," Journal of Information Systems Education, Vol. 13, No. 3, pp. 183-187.

Fitzgerald, J. & Dennis, A. (2009), Business Data Communications and Networking 10th ed., Wiley,

Mitchener, W. G. & Vahdat, A. (2001) "A Chat Room Assignment For Teaching Network Security," SIGCSE Bull. Vol. 33, pp. 31-35. http://doi.acm.org/10.1145/366413.364532

Pendegraft, N., Stone, R.W. & Byers, C.R., 2000, "Using Information Systems as a Unifying Influence in and Integrated Business Curriculum", Journal of Information Systems Education Vol. 11, No. 1&2, pp.61-66.

Rawles, P. T. & Baker, K. A. (2003), "Developing A Public Key Infrastructure For Use In A Teaching Laboratory," Proceedings of the 4th Conference on information Technology Curriculum, Lafayette, Indiana. http://doi.acm.org/10.1145/947121.947181

Reid, R. C., Platt, R. G., & Wei, J. (2005), "A Teaching Module To Introduce Encryption For Web Users," Proceedings of the 2nd Annual Conference on information Security Curriculum Development, Kennesaw, Georgia. http://doi.acm.org/10.1145/1107622.1107636

Sanders, A. (2003), "Utilizing Simple Hacking Techniques to Teach System Security and Hacker Identification," Journal of Information Systems Education, Vol. 14, No. 1, pp.5-9.

Stalling, W. (2006). Cryptography and Network Security, 4th ed., Prentice Hall, New York.

Temkin. A. (2007) "Teaching Cryptography to Continuing Education Students" IFIP International Federation for Information Processing. Vol. 237. Fifth World Conference on Information Security Education, eds. Futcher, L., Dodge, R., (Boston: Springer), pp. 121–128.

Yuan. http://yuan.ecom.cmu.edu/trapbox/, accessed 5 Sept. 2008.

Yurcik, W., & Doss, D. (2001), "Different Approaches in the Teaching of Information Systems Security, Proceedings of ISECON 2001. http://isedj.org/isecon/2001/04a/ISECON. 2001.Yurcik.pdf, accessed 5 Sept. 2008.

AUTHOR BIOGRAPHY

Norman Pendegraft is Professor of Information Systems in the College of Business and Economics at the University of Idaho. He has taught Database design and Telecommunications Management for many years. His major research interest is IS security

APPENDIX 1

Non Credit VOLUNTARY Response
Do not write your name on this paper. There is no penalty for refusing to answer.

1.To ensure privacy use _____s _____key
2. To ensure authenticity use _____'s _____key

Information Systems & Computing
Academic Professionals

STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the Journal of Information Systems Education have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

ISSN 1055-3096