Proceedings of the 12th Colloquium for Information Systems Security Education
University of Texas, Dallas
Dallas, TX June 2 - 4, 2008

What the Graduate Needs to Know about Cryptography

William Hugh Murray, *CISSP, Naval Postgraduate School*, *Verizon Business*

Abstract – ***It appears that at many, not to say, most, schools, cryptography is being taught to Computer Security and Information Assurance students by mathematicians or cryptographers. By their own reports, mathematicians and cryptographers tend to teach what interests them, even at the expense of what the student needs to know. While this may simply be a matter of pedagogy, it is often a matter of content. While the student may identify or infer for himself what he needs to know, it should not be left either to him or to chance.***

Security people need to know different things about cryptography than do cryptographers or mathematicians. It would appear that those who are teaching cryptography may not have given very much thought to what the student needs to know, as contrasted to what they would like for him to know or what they would like to teach him.

This paper attempts to identify things that users of cryptography need to know. It does so in the hope that it will encourage the teaching of these things.

Index terms – Cryptography, curriculum, encryption, cryptanalysis, key management, information assurance, data security, authentication

I. Introduction

When I was a student, there was almost no instruction in cryptography. As a matter of national policy it was a covert subject. (Indeed when I was in elementary school mathematics was a dark art.) While NSA was the largest recruiter of masters and doctors graduates in math, those graduates were not expected to know any cryptography. The new recruits were sent to the "Friedman School" where they were taught cryptanalysis. What they were taught was "classified" and they were forbidden to trade on it even if they left the Agency. When IBM needed competence in crypto, they looked to a German national, Horst Feistel.

While the policy did not officially change, the practice changed when Dr. Ruth Davis of the National Bureau of Standards agreed to publish the Data Encryption Standard. After that, the cat was out of the bag and the horse was out of the barn. While there are still no departments of cryptography in American colleges, there are courses and students; some doctorates have been awarded for work in cryptography.

At the Colloquium in Boston, by design and intent, the author sat in on a panel on teaching cryptography. It was clear that the panelists were both knowledgeable and skillful. However, as the panel went on, I found myself becoming increasingly uncomfortable with the topics that the panelists reported that they covered and with what seemed to be obvious omissions.

In my head, without benefit of paper, I had a list of topics that I would have expected to be taught. As I listened to the panel, I realized that not any of them were being reported. Admittedly, some of them were fairly subtle. On the other hand, even the most important of them were unlikely to be inferred from what was covered by even the brightest students. No student would get even a third of them by himself. Most of these things were taught in the "Friedman School."

Immediately after the completion of the panel, I began to refine and elaborate my list. Without the expenditure of very much time or effort, I came up with a fairly long list. It is beyond the role of the Colloquium to teach them. However, while I am sure that many of our colleagues will disagree, it is at least arguable that it is within our role to identify them and discuss them.

II. History

In his seminal work, The Code-breakers[i], David Kahn, traces the history of "secret writing." He recounts the "leap-frogging" through history of cryptography and cryptanalysis. He shows that new technology advances both, but, that in the long run, the advantage is always to cryptography. This reading of history is useful to advance the student's understanding of cryptography. However, it is essential to balance the belief of the young that the world has always been as they discovered it and that it does not change.

The student needs to understand that the modern computer has both increased the need for, and decreased the cost of, cryptography. It is now both ubiquitous and essential. He needs to learn that the effectiveness of cryptographic algorithms now resides in their complexity rather than in their secrecy. He needs to understand the historical significance of asymmetric key cryptography.

ISBN 1-933510-96-8

He needs to understand the power of automatic key management.

III. Applications

While the classical use of cryptography has been for confidential communication in an open and hostile environment, there are other applications that the IA student needs to know. These include:

- Hiding data at rest
- Resisting forgery
- Resisting late change
- Resisting repudiation
- Policy enforcement
- Other

Certainly the student should understand common and widely used implementations such as SSL, Kerberos, PGP, IPSec, VPNs, encrypting file systems, and full-disk encryption.

IV. Capabilities, Limitations, and Weaknesses

The cryptographer tends to focus on the weakness of algorithms. While the information assurance student relies upon the cryptographer to tell him about the limitations of his tools, what he really needs to understand is their capabilities. The way he is taught, he must infer the strength from discussion of declining strength.

V. Cryptanalysis

In the "Freidman School" the student was taught classical techniques of cryptanalysis. These included:

- Black-bag
- Brute force
- Dictionary
- Statistical
- Analytic
- Computational
- Man-in-the-middle
- Known plain-text attack
- Chosen adaptive plain-text attack (e.g., Differential Cryptanalysis)
- Other

These were taught as means of recovering an adversary's traffic. However, an understanding of these is essential not only to an understanding of cryptographic strength but also of secure use. For example, an understanding of the "known plain-text" attack helps to understand why a message should never be sent more than once and that nothing that has ever been sent in the clear should be encrypted.

Continued reports in the press about black-bag attacks against strong cryptography with weakly protected keys and long keys hidden by short pass-phrases should make it obvious that this lesson needs to be taught. (Phil Zimmerman's paper on why PGP provides only "pretty good privacy" is a good lesson.)

The student needs to understand brute force attacks in order to appreciate the issues around cover time, cost of attack, key length, key change, and the hiding of keys.

The vulnerability of the Internet to man-in-the-middle attacks makes this lesson important.

VI. Use of Strong Encryption

The student needs to understand that modern cryptography is far stronger than we need for it to be. Our algorithms are stronger than the other security mechanisms on which they rely. He needs to understand that if a forty bit key is the weak link in one's security, then one is very secure indeed. He needs to understand that to the extent that we use strong cryptography, we do so because it is cheap, not because it is necessary for security.

Similarly, the student needs to understand the difference between strong security and strong cryptography. The student needs to understand that, while modern algorithms are resistant to all but the most resourceful attacks, in practice they are no stronger than the systems and applications in which they are used. While the FBI would have us believe that "strong cryptography provides perfect security for the criminal," in fact the security is no stronger than that provided over the key or the data at the point of use (as their successful black-bag attacks have demonstrated.) As Adi Shamir says, "Attackers do not break crypto; they bypass it." The very best that cryptography can do is to move the point of attack, for example, from the network to the server, to the client.

VII. Attacks are Against the System

The student needs to understand that most attacks are against the implementation and few are against the underlying algorithm. (My mentors taught me that there are an infinite number of ways to implement an algorithm,

most of them wrong.) There will be attacks both against imperfect implementations of good ideas and against bad ideas.

It would be useful for the student to understand how implementations have been attacked in the past and why those attacks were efficient.

For example, while the Enigma mechanism is very strong, Ultra was efficient because the users encrypted known and standard headers, chose keys from a subset of the total key space, and used the same key across all traffic for an entire theater of battle for an entire day. While they changed keys daily, they distributed keys in advance.

VIII. The One-time Pad

For example, students need to understand that Shannon was silent on security. He said that a "one-time pad" yielded a perfect cryptogram, not perfect security. The student needs to understand that the one-time pad is a mathematical abstraction rather than a method of secure communications. They need to understand that Shannon was making a point about the strength of cryptograms rather than proposing a system of secure communication. The requirements of the system are so severe as to render its use impractical. Anything that one does to make it practical, results in a less than perfect cryptogram, not necessarily insecure, but not perfect.

IX. Pseudo Random Number Generators

The student needs to understand that the output of a random number generator does not yield a one-time pad. This does not mean that it is not secure for many applications, but that it does not yield a perfect cryptogram.

X. Courtney's First Law

This is a good point to say that we must remind the student that, while we can make statement, about cryptographic strength in the abstract, we can only make statements about security in the context of a specific application and environment. For example, the DES standard says that the cheapest known attack is an exhaustive attack against the key. It says nothing about whether or not it results in a cost of attack that is higher than the value of breaking one's application.

XI. Why one Cannot Roll One's own Crypto

The student needs to understand that the effort in the development of a cipher or algorithm is not in its invention but in being able to demonstrate to others anything about its strength.

Every cryptographer is familiar with the amateur who asserts that he has invented a wonderful new cryptographic algorithm that is so strong "that even he cannot break it." Often the amateur will submit a cryptogram encoded in his wonderful system and challenge the cryptographer to decode it. (He will not show the mechanism because he has not yet obtained "patent protection" for his invention.) He is usually offended when the cryptographer simply dismisses his efforts without even examining them.

What the cryptographer knows is that the effort involved in inventing a cipher pales when compared to that of being able to make any assertions about its strength. IBM, NBS, and NSA had many man years of effort behind the simple statement that the "cheapest known attack against the DES is an exhaustive attack against the key." Thirty years later that statement remains true.

The cryptographer will not give the amateur effort more than a cursory glance because he understands how much effort is involved. He will not try to decode the cryptogram because it is not big enough to contain enough information to expose weaknesses. While he suspects that he could easily find weaknesses in a disclosed mechanism, he will not spend any effort on an undisclosed or unknown mechanism.

XII. The DES is not "Broken"

The student needs to understand that the press uses the term "broken" in a very casual way; often cryptographers are not much better.

For example, in 1991 Eli Biham and Adi Shamir published their seminal paper on **Differential** Cryptanalysis of **DES**-like Cryptosystems[ii]. This paper resulted in two articles in the New York Times. The first, by John Markoff, was headlined "DES Broken." The second, by Gina Kolado, said "What do NSA and IBM know (about selecting s-boxes) that the rest of us do not?" Kolada's article was correct while Markoff's headline was misleading. As noted above, the cheapest known attack against the DES is a brute force attack against the key; that is all that was ever claimed for it.

(To their credit, Biham and Shamir made no claim that DES was broken Rather, what they showed was that the

complexity of the DES might be somewhat less than had previously been thought. (IBM confirmed their conclusion.) They showed that if one had beneficial use of the key for a very long time, but no other knowledge of it, one could discover it using only cryptanalysis in less than 2^56 operations. While this did not reduce the cost of a practical attack, it was enlightening. They showed that the DES was sensitive both to the number (16) of iterations (rounds) and to the selection of the s-boxes. (To do this they had to reinvent a method of cryptanalysis which the NSA had "classified" and IBM had agreed to keep secret.)

XIII. What does it mean to say that an Algorithm is Broken?

Does it mean:

1. The mechanism is no longer useful for any purpose?
2. The cost of recovering the clear text without benefit of the key has fallen to zero?
3. The cost has dropped to the cost of encryption?
4. The cost has fallen to equal to or less than the value of the data or the next least cost attack?
5. The cost has fallen to within several orders of magnitudes of the cost of encryption or the value of the data?
6. The elapsed time of attack has fallen to within magnitudes of the life of the data, regardless of the cost thereof?
7. The cost has fallen to less than the cost of a brute force attack against the key?
8. Someone has recovered one key or one message?

Certainly if 1, 2, or 3 were achieved, that would clearly constitute a break. On the other hand, the cryptanalyst would argue that it is broken long before that; otherwise there would be little to talk about. There has been no algorithm in history where the cost of attack suddenly fell to the cost of encryption, much less to zero. While, if one uses modern computers, the cost of breaking a simple substitution cipher is close to the cost of encryption, that result took centuries. It is still not zero. While it was predictable, the very prediction gave time for the development of alternatives. The theory, while sometimes held only by the princes, has always anticipated the practical application by years or even decades.

While one might likely consent that 4 constitutes a "break," nothing like that has happened in modern times. Indeed, by that test Enigma still stands pretty tall. The cryptanalyst would insist that 5 constitutes a break. Thus, when RSA 129 was recovered it was reported as a "break" even though the cost of doing so was 5000 MIPS years and the value of the data only $100-. It was an interesting demonstration but no one would repeat it for the money or the fun. (If he had had to use his own money, it is unlikely that the analyst would have done the experiment in the first place.)

From a security point of view a cryptographic mechanism is not broken until you get to definition 4; one does not even become concerned until one gets to 5. While not all attackers are rational and some will spend more to break a code than it is worth to do so, on average most are rational. They may spend a dime to make nine cents, but they will not willingly and deliberately do it over and over.

Even if attackers are not rational, we security people are. We love mechanisms like cryptography where the difference in cost between highly effective and gross overkill is so small and shrinking so fast. I guarantee you that IA professionals know how to use such a mechanism effectively.

XIV. Feasible v. Efficient

We should teach our students to distinguish between feasible attacks and efficient ones. The cryptographer may dismiss an algorithm once he concludes that an attack is feasible. The security practitioner can continue to use it until such an attack is efficient in his application and environment.

For example, with frequent and automatic key change, the DES is still efficient for protecting the routine financial transactions for which it was developed.

XV. The Advantage of Wholesale Cryptanalysis

We often talk about the ability of the government to read our traffic. The student should understand that those, like nation states, that do cryptanalysis on a very large scale, have a much lower cost of attack per message or other object than other adversaries. Indeed, one might conclude that NSA can read any traffic that it wants to. However, it cannot read read all the traffic that it might want. In comparing the cost of attack of a nation state to the value of breaking his application, the information assurance student needs to understand that the cost to the nation state of reading his traffic includes the value of the messages that were foregone to read his.

XVI. Hashes

As with cryptographic algorithms, the cryptographer tends to focus on the limitations of hashing algorithms,

specifically collisions. The information assurance student needs to understand that collisions are inevitable. The issue is not whether or not collisions can occur but how difficult it is to exploit them. He also needs to understand the power of multiple hashes, signatures, and time stamps to resist forgeries.

XVII. Key Management

Perhaps the most under covered area in the field is that of Key Management. No matter how well the student understands algorithms, if he does not understand key management, then he will not achieve the intended result. Information assurance students need to understand the uses and applications of key management including:

- Enforcement of policy
- Separation of roles and duties
- Resisting repudiation
- Compensation for limitations of algorithms
- Increasing cost of attack and reducing value of success by frequent change (increasing effective key-length)
- Other

He needs to understand the functions of key management including:

- generation
- recording
- transcription
- distribution
- installation
- storage
- change
- disposition
- control
- other

He needs to know that the IBM developers of modern key management believe that their most significant idea was that of the "key control vector," meta data about the key that enabled them to specify and control its use.

He needs to understand the principles of key management[iii] including:

- No key may ever appear in the clear
- Keys must be chosen evenly from the entire key space
- Therefore keys should be randomly generated by a secure engine
- Key-encrypting keys must be separate from those keys used for other objects
- Everything encrypted under a key-encrypting key must originate within a crypto engine
- Key management must be fully automated and independent of the user

XVIII. Conclusion

This paper is based upon no better authority than the observations and opinions of the author. However, the author has more than four decades of experience in the field; he has earned the right to his opinion and has a duty to share it. It is a response to what a panel of faculty reported to the Colloquium, rather than research across a large sample of programs. However, this is what the Colloquium is for.

One possible response to this list is that it needs to be elaborated and defended. Reviewers complained that there is not a single source that one can turn to that treats them all. I am really sorry about that. Can we consider this a start? If I wrote the book, would you buy it?

The reader may be tempted to dismiss these topics as so obvious that they do not need to be covered. In fact they are not obvious and there are few faculty members who could teach them all without additional preparation. Some of these topics are fruitful topics for research.

Finally, the security student needs to learn about cryptography that, while cryptography does have limitations, its economics are always on his side. While his costs rise linearly, those of his adversary rise exponentially.

XIX. References

[i] ***THE CODEBREAKERS:*** D Kahn, *Macmillan 1967, Library of Congress catalog no. 63-16109*

[ii] Eli Biham, Adi Shamir, **Differential Cryptanalysis of DES-like Cryptosystems**, Technical report CS90-16, Weizmann Institute of Science CRYPTO'90 & Journal of Cryptology, Vol. 4, No. 1, pp. 3-72, 1991.

iii C. H. Meyer , S. M. Matyas, **Some cryptographic principles of authentication in electronic funds transfer systems**, Proceedings of the seventh symposium on Data communications, p.73-88, October 27-29, 1981, Mexico City, Mexico