Ethical Issues in Cryptography and Information Security:

Concerns for Digital Libraries

By

Arifa. K.

Senior Research Fellow

Dept. of Library and Information Science

University of Calicut

Calicut - 673635

ABSTRACT

Cryptography has widely been used as a means of information security in today's electronic world. In addition to e-commerce, e-mail and other applications over the Internet, it has been used in common household items as well. The increased reliance on cryptographic methods has raised several ethical questions of global concern that are closely related to fundamental human rights. Some view it as a boon, as an escape from the oppressive hands of the state while others see it as a way of making the information - poor have to pay for every information and denial of access to essential information. In this paper an attempt has been made to separate out the concepts appropriate to each interpretation. Digital libraries also face quite many ethical problems concerning cryptography that even stand against the principles of a public library system. The problems are related to inequality of access, intellectual property and copyright issues.

KEYWORDS: Cryptography, Information Security, Digital Libraries

0. INTRODUCTION

Today, almost everything can be considered as having an ethical dimension. Ethics have now been applied to technological options as well which include the ethics of encryption and decryption- i.e. cryptography. The use of cryptography in digital network environment raises numerous open legal and ethical issues that need to be solved on the international level. There exist many controversial questions regarding cryptography and information security that will have a large influence on the ways we conduct business and access information. Information may be owned but in way that is distinct from material property ownership .It may be withheld from, or conversely forced upon citizens .There may be a right to know –like privacy issues, freedom of information aspects, especially from governments and essential information like health information. While considering the ethical side of cryptography, we are not concerned about what technology is; but what we are considering is the ethics of a process that renders information useless unless you have a 'key'. This paper focuses on the ethical issues related to encryption of information and ethical concerns for the emerging digital libraries.

1. CRYPTOGRAPHY-WHY IS IT IMPORTANT?

Before getting to the ethical aspect it would be apt to know what cryptography means, why it is so important. Cryptography, today might be summed up as the study of techniques and applications that depend on the existence of difficult problems. To most people, cryptography is concerned with keeping communications private, though it is only the part of today's cryptography. Encryption is the transformation of data into a form that is as close to impossible as possible to read without the appropriate knowledge (a key). Its purpose is to ensure privacy by keeping information hidden from any one for whom it is not intended, even those who have access to the encrypted data. Decryption is the reverse of encryption-it is the transformation of encrypted data back into an intelligible form. Encryption and decryption generally require the use of some secret information, referred to as key .For some encryption mechanisms, the same key is used for both encryption and decryption; for other mechanisms, the keys used for encryption and decryption are different.

Today's cryptography is more than encryption and decryption. Authentication allows one to have more confidence in his electronic transactions than in real life transactions. As we move to a world were our decisions and agreements are communicated electronically, we need to have electronic techniques for providing authentication. Cryptography provides mechanisms for these-digital signature binds a document to the possessor of a particular key, while a digital timestamp binds a document to its creation at a particular time. The field of cryptography encompasses other uses as well. With a just few basic cryptographic tools, it is possible to build elaborate schemes and protocols that allow us to pay using electronic money, to prove that we know certain information without revealing the information itself and to share a secrete quantity in such a way that the subset of shares can reconstruct the secret.

The importance of cryptography lies in that it allows people to carry over the confidence found in the physical world to the electronic world, thus allowing people to do business electronically without worries of deceit and deception. Every day hundreds of thousands of people interact electronically, whether it is through e-mail, e-commerce, ATM machines or cellular phones. The perpetual increase of information transmitted electronically has led to an increased reliance on cryptography. Over the Internet, cryptography makes secure website and electronic safe transmissions possible. For a website to be secure, all of the data transmitted between the components where data is kept and where it is received must be encrypted. This allows people to do online banking, online trading and make online purchase with their credit cards, without worrying that any of their account information is being compromised. Cryptography is very important to the continued growth of Internet and electronic commerce. E-commerce, which is increasing at a very rapid rate, the commercial transactions on the Internet are expected to total hundreds of billions in a year. This level of activity could not be supported without cryptographic security. E-mail, which is now used by people to conduct personal and business matters on a daily basis, has no physical form, and may exist electronically in more than one place at a time. This poses a potential problem from eavesdroppers. Encryption protects e-mail by rendering it very difficult to read by an unintended party. Digital signature, which can also be used to authenticate the origin and content of an e-mail message, are built using the contents of the documents being signed, and so falsification of any kind becomes very difficult. Cryptography is also used to regulate access to satellite and cable T. V., Cable T. V. is set up so people can only watch the channels they pay for. Pay-per-view cable allows cable subscribers to 'rent' a movie directly through the cable-box, what the cable box does in decode the incoming movie, but not until the movie has been 'rented'. The satellite TV companies, to alleviate the problem of people getting free T. V., use cryptography by allowing only those who paid for their service to unscramble the transmission by using receivers.

We see that cryptography is widely used, not only is it used over the internet, but also it is used in phones, televisions, and a variety of other common household items. Without cryptography, hackers could get into our e-mail, listen to our phone conversation, tap into our cable companies and acquire free cable service or break into our bank/ brokerage accounts.

2. THE ETHICS OF CRYPTOGRAPHY AND INFORMATION SECURITY

Encryption systems are in most cases praised as an essential component in human self-determination, where encryption is felt to offer an escape from the oppressive hands of the state. In other cases it is seen as a way of making the information dearer "pay before they play" – a system of denial of access to specific information that is essential to human development. Although the systems based on encryption has always seemed like a good idea, it has also brought about some chaos. With encryption, we often have the same people arguing in opposite directions depending on the context. The ethical issues in cryptography pose equations basically on rights – on individual freedoms, on individual access and the ultimate question of to track or not to track.

2.1 Cryptography and Individual freedoms

2.1.1 Is it that my key protects the privacy of my communications?: This is quite a matter of government vs. public interests. The state imposing strong cryptography on the national infrastructure with the citizens having to do with weaker versions and none allowed to export the strong brew, the condition brings about opposing groups – one voicing for the state and the other for the citizens. The US. Government's role in restricting the use and export of powerful encryption technology has brought about serious debate between libertarians and Big Brother. There are contending views among the first group about the key escrow or key recovery encryption where the encryption keys are stored with 'trusted third parties' or TTP's. One group argues that the key escrow is the best way to regulate access. The other group is of the view that critical infrastructure are rendered more vulnerable to attack, allowing the third parties, however trusted, to have access to the encoded communication.

On the other side, those standing for the citizens argue that the citizens have the right to encrypt their message using the strongest encryption, that no one and particularly the government can read them. Those who are of this view cannot accept the storage of encryption keys, nor key escrow with the government. They do not even trust the notion of key escrow with a trusted third party or any outside body responsible to the government. There are numerous questions they ask to support their view.

If some governmental watchdog authority can gain access to the key simply by presenting a suitable warrant, then what is the use of the key?

Who will watch the watchdog then?

Can one be sure that the criteria set by the state for the 'need to know' will not be at an arbitrarily low level?

Will the encrypted private documents be compulsory decrypted only for suspected serious crime; will they also be decrypted in pursuit of individualistic, even socially deviant behaviour?

All these are questions of ethical concern where the citizen's right to encryption is presented as an aspect of individual morality. The European commission is of the view that privacy considerations suggest not to limit the use of cryptography as a means to ensure data security and confidentiality.

2.1.2 Is it that their key prevents my access to information about me?: This relates to the state restricting the private citizens's freedom of access to information about themselves. There are ethical aspects in the existence and deployment of encryption for the purpose of state secrecy. Information acts in very few countries do legislate the access of citizens to information about themselves and about the workings of the state. But most countries in the world do not have such provisions and it is in the hands of these governments that powerful encryption can be and they use it as a means to hide information that the state does not want to expose to the public.

2.2 Cryptography and individual access

The question of individual access involves intellectual property, copyright issues and access to essential information.

2.2.1 Is it that my key protects my intellectual property?: The materials that one creates in the electronic media are his own intellectual property and by encrypting it he is protecting his property from theft and tampering. He is protecting his moral rights of integrity and paternity, while helping the users by ensuring the authenticity of his content and providing a warranty for his authorship. Those who argue that access to intellectual property should be free of cost and regulation by legal instruments like copyright law likes to characterize their adversaries as wealthy rights holders. Publishers, producers and broadcasters who run this argument are demanding high profit – margins and thus creating undemocratic separations of people into information rich and information poor. But it is a fact that original creators of all the content are not publishers or producers, but individual authors and artists. If the content being made cost-free and copyright law is not enforced, an impulse for much of the creation will be removed. Moreover, most of the creators are not so wealthy and are rarely adequately compensated for the time and effort they put into their creations.

An obvious problem with encryption as a global solution is that once something has been decrypted by an authorized user, it may also be vulnerable to trangressive copying and tampering. This requires that decryption should take place in a secure environment and in a

transient way. Thus in environments like the Internet, encryption cannot be seen as the ideal way to protect some forms of content. In other circumstances like digital broadcasting, where the risk of the decoded signal being emitted further does not exist in a single emitter/many receiver model, encryption serves the purpose effectively. However, the ethical aspect lies in using encryption to withhold information in circumstances where information is critical to human development. Different ethical questions surround the issue of free access and freedom of access to information. The first one is rather an economic question, which relates to the price of information and the latter relates to the price of information and the latter relates to the barriers to accessing information.

2.2.2 Is it that their key prevents my access to essential information? The question of access tends to bring forward the ideas of information rich and information poor- the bye product of the global Information technology revolution. Essential information is the information related to the basic minimum needs of the humanity. It can be considered to be the information essential to the development of backbone industries, basic science, and survival in health, education, welfare and labour. The matter of essential information poses many ethical questions. With the gradual encryption of valuable information, the so-called information poor who are backward in all senses are denied the access to essential information. The masses of low-income classes like students throughout the world and their libraries will be unable to afford the high quality and timely electronic information.

Essential information is disseminated by broadcasting. One of the main models applied is advertising-sponsored broadcasting. Viewers receive high-value or high price information that is fully subject to copyright and other intellectual property conditions at the cost of being subjected to advertising at regular intervals-nevertheless it provides for a democratic method for disseminating content and proves to be highly beneficial for the information poor. Internet, which has more than a broadcasting environment with many-to-many interconnections, will prove quite helpful, if these kinds of methods are commended. However, any system, which requires to “pay before you play”, will exclude those who cannot afford the access price, and in any developing country with meagre income, any access price is going to be too high. In this context, the role of encryption and the ethical question related to it is that of the access right to essential information. Materials, if encrypted and then decrypted in secure environments after the users pay the entry price, are clearly valuable for specific contents like a patented formula. But if such measures are adopted as standards, the threat is that essential information will also be encrypted and placed out of the reach of information poor even if there is zero access prices.

2.3 To track or not to track?

Another point of ethical concern is whether the legitimate pursuit of rights infringes the rights to privacy of those whom you are pursuing.

2.3.1 Tracking tells them what I am doing: Digital watermarking, where the watermark is encrypted and where rights management information is placed in the watermark, the rights holder should be able to track their works throughout the Internet. The first concern is that the right to track the location of specific content could be abused by authoritarian forces. It is certainly an invasion of privacy to seek and gain accurate and consistent information about what an individual is reading, viewing, hearing or feeling. One’s senses are his private property.

2.3.2 Tracking tells me who is ripping me off: Tracking can provide information about piracy, about attacks that damage the authenticity or integrity of the work and about infringement of moral rights. The creator wants to know this as much as the user wants guarantees of an integral authentic text. This dilemma is quite of concern, the solution to this would appear to lie in systems that only track the unauthorized uses i.e., you may look where the work is not supposed to be, rather than where the work is lawfully stored.

3. ETHICAL CONCERNS FOR DIGITAL LIBRARIES

Ethical aspects are pervading question for digital libraries. The ethical concerns of cryptography revolves around the intellectual property and copyright issues and hence a matter of information access. In fact, cryptography seems to be the basis for implementing copyright and access authorization in digital environments. It can provide new means of protecting intellectual property in the digital world. But the important ethical issue concerning libraries is-should there be free copies of information available for lend in the libraries? If so, what prevents all users from taking a free copy of the work? Why would anybody then pay for the information?

Moreover, payment for every access to a particular piece of information is against the principles of public library systems that are based on free and fair use. It would be quite difficult to refer to scientific facts, if checking or making a reference costs money. Thus the pay-per –use method may deter learning and research work. However, the information when made totally free of cost will pose problems as discussed earlier. It can also most probably lead to overuse, imbalances and access restriction based on allocation rules. It may also lead to reduction in quality. However, it is quite demanding to find a balance between author/publisher interest in receiving compensation and the user /library interests in having access to information on fair and reasonable terms. A strict pay-per use method is unlikely to succeed fully. License based arrangements can solve the problems to some extent.

4. CONCLUSION

Thus we see that the role of encryption in protecting individual freedom is based on the notion that an individual should be able to make use of powerful encryption technology to protect the privacy of his personal communications. The chaos lies in that those who argue for this at the same time oppose being denied access to information held by themselves by the same technology. Most of us criticize the iniquity of encryption in preventing the information poor from gaining access to essential information. But it should be that those who create intellectual property (authors, artists etc) should be able to use techniques including encryption, to protect their creations from tampering and also to earn a living from their creativity. Systems that combine unencrypted content with identification information held in digital watermarks provide hopes of a solution to these two views. Law is an efficient weapon against tampering or piracy and the identification information is used as the evidence of ownership.

REFERENCES

1. Samuelson, Pamela. Copyright and Digital Libraries, *Communications of the ACM,* 38. 4, p110.

2. Zwass, V. Ethical issues in Information Systems. In: Encyclopedia of Library and Information Science, 57 supplement 20, p175

3. COST-Computer Security Technologies. www HomePage.

4. John,N (1998). Libraries and Global Information Infrastructure.

http: // www. unesco. org/webworld/ infoethics-2/eng/proceedings.htm.

5. Security and cryptography links. http://www.semper.org/sirene/outside world/9620 security. html.

BRIEF BIOGRAPHY OF AUTHOR

Arifa K. is a Research Scholar at Department of Library and Information Science, University of Calicut, Kerala. She holds B.Sc in Physics and M. L .I. Sc. At present working on the final thesis.