ISSN 2319 – 7757 EISSN 2319 – 7765

Indian Journal of Engineering

The enormous security technique: cryptography

Nikita Chhillar[1], Preeti Dhanda[2], Nisha Yadav[3], Nisha Yadav[4], Shikha Yadav[5]

1. Department of Computer Science and Engineering, Dronacharya College of Engineering, Khentawas, Farukhnagar, Gurgaon, India, Email: nikitachhillar@yahoo.com
2. Department of Computer Science and Engineering, Dronacharya College of Engineering, Khentawas, Farukhnagar, Gurgaon, India, Email: preeti.dhanda01@gmail.com
3. Department of Computer Science and Engineering, Dronacharya College of Engineering, Khentawas, Farukhnagar, Gurgaon, India, Email: jazzynishu@gmail.com
4. Department of Computer Science and Engineering, Dronacharya College of Engineering, Khentawas, Farukhnagar, Gurgaon, India, Email: yadav.nisha2993@gmail.com
5. Department of Computer Science and Engineering, Dronacharya College of Engineering, Khentawas, Farukhnagar, Gurgaon, India, Email: yadav21shikha@gmail.com

Received 26 October; accepted 19 November; published online 01 December; printed 16 December 2012

ABSTRACT

There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords. One essential aspect for secure communications is that of secret key cryptography, which the focus of this paper. With secret key cryptography, a single key is used for both encryption and decryption. The key selection mechanism and the encoding methodology express the efficiency of the cipher text generated. In this paper, a new method of encoding technique using the mathematical operators over Unicode character set facilitates better encoding algorithm.

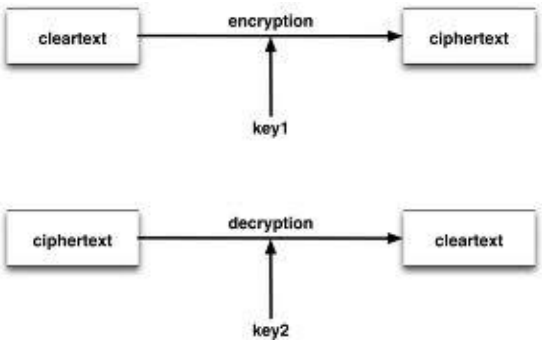
KEYWORDS: pc, pkcs, prng, crpto.

1. INTRODUCTION

Cryptography is where safety engineering meets mathematics. It provides us with the tools that underlie most modern security protocols. It is probably the key enabling technology for protecting distributed systems. Cryptography has often been used to, protects the wrong things, or used to protect them in the wrong way. Unfortunately, the computer security and cryptology communities have drifted apart over the last 20 years. Security people don't always understand the available crypto tools, and crypto people don't always understand the real-world problems. There are a number of reasons for this, such as different professional backgrounds (computer science versus mathematics) and different research funding (governments have tried to promote computer security research while suppressing cryptography). The basic terminology is that cryptography refers to the science and art of designing ciphers; cryptanalysis to the science and art of breaking them; while cryptology, often shortened to just crypto, is the study of both. The input to an encryption process is commonly called the plaintext, and the output the cipher text. There are a number of cryptographic primitives—basic building blocks, such as block ciphers, stream ciphers, and hash functions. Block ciphers may either have one key for both encryption and decryption, in which case they're called shared key (also secret key or symmetric), or have separate keys for encryption and decryption, in which case they're called public key or asymmetric.

2. HISTORY

Before the modern era, cryptography was concerned solely with message confidentiality (i.e., encryption) — conversion of messages from a comprehensible form into an incomprehensible one, and back again at the other end, rendering it unreadable by interceptors or eavesdroppers without secret knowledge (namely, the key needed for decryption of that message). In recent decades, the field has expanded beyond confidentiality concerns to include techniques for message integrity checking, sender/receiver identity authentication, digital signatures, and interactive proofs and secure computation, amongst others. The earliest forms of secret writing required little more than local pen and paper analogs, as most people could not read. Essentially, prior to the early 20th century, cryptography was chiefly concerned with linguistic and lexicographic patterns. Since then the emphasis has shifted, and cryptography now makes extensive use of mathematics, including aspects of information theory, computational complexity statics, combinatory, abstract algebra and number theory. Cryptography is, also, a branch of engineering, but an unusual one as it deals with active, intelligent, and malevolent opposition most other kinds of engineering need deal only with neutral natural forces. There is also active research examining the relationship between cryptographic problems and quantum physics.



3. WHAT IS CRYPTOGRAPHY?

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient.

4. WHAT IS A CRYPTOGRAPHIC ALGORITHM?

A cryptographic algorithm, or cipher, is a mathematical function used in the encryption and decryption process. A cryptographic algorithm works in combination with a key (a number, word, or phrase) to encrypt and decrypt data. To encrypt, the algorithm mathematically combines the information to be protected with a supplied key. The result

Nikita chhillar et al.
The enormous security technique: cryptography,
Indian Journal of Engineering, 2012, 1(2), 105-107,

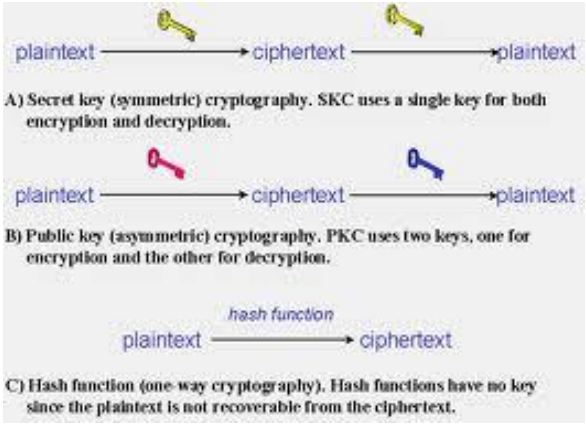
of this combination is the encrypted data. To decrypt, the algorithm performs a calculation combining the encrypted data with a supplied key. The result of this combination is the decrypted data. If either the key or the data is modified, the algorithm produces a different result. The goal of every encryption algorithm is to make it as difficult as possible to decrypt the generated cipher text without using the key. If a really good encryption algorithm is used, then there is no technique significantly better than methodically trying every possible key. Even for a key size of just 40 bits, this works out.

5. THE ONE-TIME PAD

Plain: heilhitler Key: wclnbtdefj Cipher:DGTYIBWPJA	Cipher: DGTYIBWPJA KEY: wggsbtdefj Plain: hanghitler	Cipher: DCYTIBWPJA KEY: wclnbtdefj Plain: hanghitler
Figure x To entrap the spy	**Figure y** What the spy claimed he said	**Figure z** Manipulating the message in

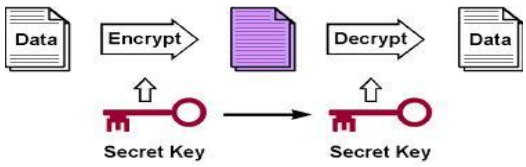
One way to make a stream cipher of this type proof against attacks is for the key sequence to be as long as the plaintext, and to never repeat. This was proposed by Gilbert Vernam during World War I; its effect is that given any cipher text and any plaintext of the same length, there is a key that decrypts the cipher text to the plaintext. Regardless of the amount of computation that opponents can do, they are wiser, as all possible plaintexts are just as likely. This system is known as the one-time pad. Leo Marks' engaging book on cryptography in the Special Operations Executive in World War II relates how one-time key material was printed on silk, which agents could conceal inside their clothing; whenever a key had been used, it was torn off and burned. An example should explain all this. Suppose you had intercepted a message from a wartime German agent, which you knew started with "Heil Hitler," and that the first 10 letters of cipher text were DGTYI BWPJA. This means that the first 10 letters of the onetime pad were wclnb tdefj, as shown in Figure x. Once he had burned the piece of silk with his key material, the spy could claim that he was actually a member of the anti-Nazi underground resistance, and that the message actually said "Hang Hitler." This is quite possible, as the key material could just as easily have been wggsb tdefj, as shown in Figure y. Now, we rarely get anything for nothing in cryptology, and the price of the perfect secrecy of the one-time pad is that it fails completely to protect message integrity. Suppose that you wanted to get this spy into trouble; you could change the cipher text to DCYTI BWPJA, as shown in Figure z. During the World War II, Claude Shannon proved that a cipher has perfect secrecy if and only if there are as many possible keys as possible plaintexts, and if every key is equally likely; therefore, the one-time pad is the only kind of system that offers perfect secrecy. The one-time pad is still used for high-level diplomatic and intelligence traffic, but it consumes as much key material as there is traffic, hence is too expensive for most applications. It's more common for stream ciphers to use a suitable pseudorandom number generator to expand a short key into a long key stream. The data is then encrypted by exclusive-or'ing the key stream, one bit at a time, with the data. It's not enough for the key stream to appear "random" in the sense of passing the standard series randomness tests; it also must have the property that an opponent who gets their hands on even a number of key stream bits should not be able to predict any more of them. Stream ciphers are commonly used nowadays in hardware applications where the number of gates has to be minimized to save power.

6. TYPES OF CRYPTOGRAPHIC FUNCTIONS



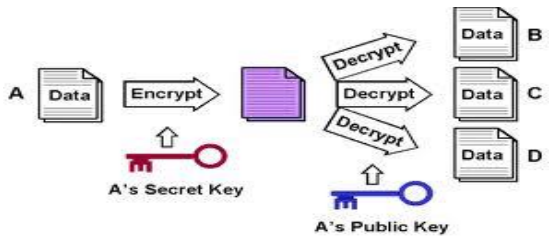
There are three kinds of cryptographic functions: hash functions, secret key functions, and public key functions. We will describe what each kind is, and what it is useful for. Public key cryptography involves the use of two keys. Secret key cryptography involves the use of one key. Hash functions involve the use of zero keys! Try to imagine what that could possibly mean, and what use it could possibly have—an algorithm everyone knows with no secret key, and yet it has uses insecurity.

7. SECRET KEY CRYPTOGRAPHY



Secret key cryptography involves the use of a single key. Given a message (called plaintext) and the key, encryption produces unintelligible data (called an IRS Publication—no! no! that was just a finger slip, we meant to say "cipher text"), which is about the same length as the plain text was. Decryption is the reverse of encryption, and uses the same key as encryption.Secret key cryptography is sometimes referred to as conventional cryptography or symmetric cryptography. The Captain Midnight code and the monoalphabetic cipher are both examples of secret key algorithms, though both are easy to break.

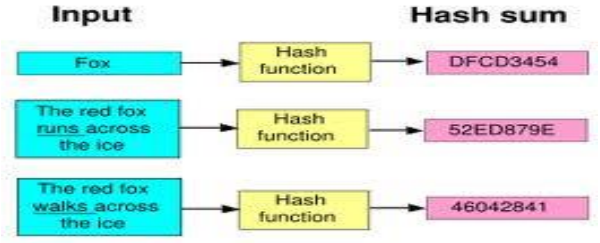
8. PUBLIC KEY CRYPTOGRAPHY



Public key cryptography is sometimes also referred to as asymmetric cryptography. Public key cryptography is a relatively new field, invented in 1975 [DIFF76b] (at least that's the first published record—it is rumored that NSA or similar organizations may have discovered this technology earlier). Unlike secret key cryptography, keys are not shared. Instead, each individual has two keys: a private key that need not be revealed to anyone, and a public key that is preferably known to the entire world. Note that we call the private key a private key and not a secret key. This convention is an attempt to make it clear in any context whether public key cryptography or secret key cryptography is being used. There are people in this world whose sole purpose in life is to try to confuse people they will use the term secret key for the private key in public key cryptography, or use the term private key for the secret key in secret key technology. One of the most important contributions we can make to the field is to convince people to feel strongly about using the terminology correctly—the term secret key refers only to the single secret number used in secret key cryptography. The term private key MUST be used when referring to the key in public key cryptography that must not be made public. (Yes, when we speak we sometimes accidentally say the wrong thing, but at least we feel guilty about it.) There is something unfortunate about the terminology public and private. It is that both words begin with p. We will sometimes want a single letter to refer to one of the keys. The letter p won't do. We will use the letter e to refer to the public key, since the public key is used when encrypting a message. We'll use the letter d to refer to the private key, because the private key is used to decrypt a message. Encryption and decryption are two mathematical functions that are inverses of each other. There is an additional thing one can do with public key technology, which is to generate a digital signature on a message.

Nikita chhillar et al.
The enormous security technique: cryptography,
Indian Journal of Engineering, 2012, 1(2), 105-107,

9. HASH FUNCTIONS



Hash functions, also called message digests and one-way encryption are algorithms that, in some sense, use no key Instead; a fixed-length hash value is computed based upon the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered. Hash algorithms are typically used to provide a digital fingerprint of a file's contents often used to ensure that the file has not been altered by an intruder or virus. Hash functions are also commonly employed by many operating systems to encrypt passwords. Hash functions, then, provide a measure of the integrity of a file.

10. THE BENEFITS OF CRYPTOGRAPHY

- A broad range of asymmetric (public key) algorithms, symmetric (secret key) ciphers and message digests provides flexibility for a wide variety of security needs.
- Random number generation via a pseudo-random number generator (PRNG) and the FIPS 186-2 PRNG.
- Key generation services automate key generation and provide for the creation of cryptographic keys
- Cryptographic syntax and data encoding services comply with public key cryptography standards (PKCS) for more seamless interoperability.
- Memory management and protection services provide more control of the memory allocated to hold the output of large calculations, providing more flexibility.
- High-speed math processing provides great performance in calculations of large numbers - especially critical in public key operations - saving valuable time.
- Native code services provide the ability to use native C code for improved performance.
- Memory obfuscation to protect sensitive data when not in use and byte code obfuscation to prevent the unauthorized use of sensitive methods and classes.
- Cryptographic techniques offer three essential types of services for electronic commerce: authentication (which includes identification), non repudiation, and privacy. Identification, a sub-type of authentication, verifies that the sender of a message is really who he or she claims to be. Authentication goes a step further- verifying not only the identity of the sender, but also that the message sent has not been altered. Non- repudiation is an important requirement in commercial transactions, it's implementation prevents anyone from denying that they sent or received a certain file or data, and is similar to sending a letter certified and return receipt requested through the United States postal service. Finally, privacy is the ability to shield communications from unauthorized viewing.

11. CONCLUSION

The conclusion of this paper is that cryptography has been proved as a very important aspect in the network security nowadays. We can easily send our secret data and confidential data over networks. The basic properties the safety trick needs to understand are not too difficult to grasp, though there are some subtle things that can go wrong. In particular, it is surprisingly hard to build systems that are robust even when components fail (or are encouraged to), and where the cryptographic mechanisms are well integrated with other measures such as access control and physical security.

REFERENCES

1. An Efficient Operator based Unicode cryptography Algorithm" for Text,Audio and Video Files by R.Sumathi and R. Sundarrajan
2. "Chaos-Based Cryptography: A Brief Overview" by Ljupc˘o Kocarev*
3. M. Bellare, Z. Brakerski, M. Naor, T. Ristenpart, G. Segev, H. Shacham and S. Yilek. "Hedged Public-Key Encryption"
4. Cryptography *ZHQM ZMGM ZMFM* —G. JULIUS CAESAR

Nikita chhillar et al.
The enormous security technique: cryptography,
Indian Journal of Engineering, 2012, 1(2), 105-107,