CIT 270: SYSTEMS SECURITY I

CHAPTER 3: BASIC CRYPTOGRAPHY

BYU IDAHO

INTRODUCTION

Remember this presentation does not replace your reading and only covers at best 70% of the chapter material.

Note

Keep any eye out for boxes like this one in your chapter readings. These are note boxes that highlight important information. Your chapter quiz will often have questions that refer directly to one of these.

In this presentation pay special attention to yellow words. These highlighted words denote a topic that will almost always be on your chapter quiz.

DEFINING CRYPTOGRAPHY

Cryptography comes from the Greek words meaning *hidden writing*. It is the practice of transforming (encrypted / scrambling) information so that it is secure and can not be accessed (decrypted / unscrambled) by an unauthorized party.

Steganography: the practice of hiding the existence of data.

Encryption: the process of changing the original text into a scrambled message

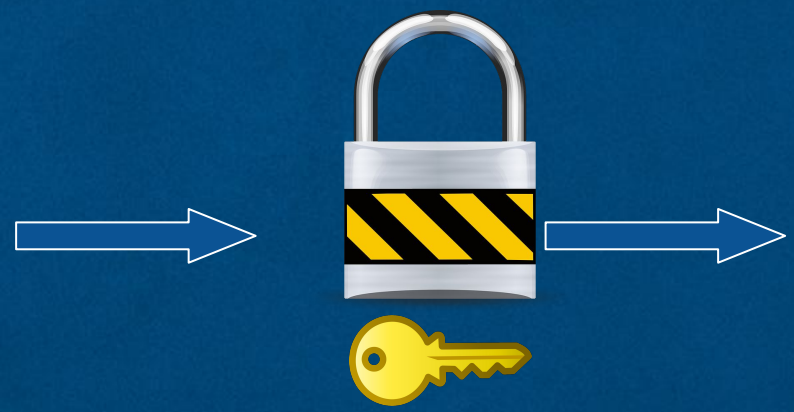
Algorithm aka. Cypher: the process by which data is encrypted or decrypted using mathematical formulas.

DEFINING CRYPTOGRAPHY

Plaintext

Confidential Memo:

Layoffs at the Lakeview store will happen next week.



Ciphertext

LXF3!OP7VE7FR
NHR9A@U11E62
6VSCC#P0$12AH

DEFINING CRYPTOGRAPHY

Ciphertext

LXF3!OP7VE7FR
NHR9A@U11E62
6VSCC#P0$12AH

Decryption Algorithm

Key

Plaintext

Confidential Memo:

Layoffs at the Lakeview store will happen next week.

DEFINING CRYPTOGRAPHY

There are many different categories of algorithms, two common types are the:

1. Substitution Cipher where one character is substituted for another character. ROT13 is one type of substitution (Caesar) cipher.

2. XOR Cipher is based on the binary operation eXclusive OR (XOR / ^) that compares two bits against each other. If the bits are different 1 is returned and if the bits are identical then a 0 is returned.

DEFINING CRYPTOGRAPHY

ROT13 / Caesar Cipher

XOR Cipher

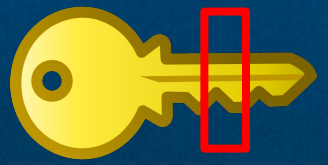
DEFINING CRYPTOGRAPHY

Software relies on Pseudorandom Number Generators (PRNG). PRNG are an algorithm for creating a sequence of numbers whose properties approximate those of a random number.

Diffusion is one way to thwart statistical analysis by insuring that a single character change in the plaintext changes multiple characters of the ciphertext.

Confusion is another way to thwart statistical analysis by insuring the key does not relate in a simple way to the ciphertext.

1 = 1



1 to many

DEFINING CRYPTOGRAPHY

Cryptography can provide a range of software protections such as:

- Confidentiality
- Integrity
- Authentication
- Non-repudiation
- Obfuscation

DEFINING CRYPTOGRAPHY

Cryptography can provide a range of software protections such as:

- Confidentiality
- Integrity
- Authentication
- Non-repudiation
- Obfuscation

Only Authorized people can view the data or message.

DEFINING CRYPTOGRAPHY

Cryptography can provide a range of software protections such as:

- Confidentiality
- Integrity
- Authentication
- Non-repudiation
- Obfuscation

The data is correct and unaltered.

DEFINING CRYPTOGRAPHY

Cryptography can provide a range of software protections such as:

- Confidentiality
- Integrity
- Authentication
- Non-repudiation
- Obfuscation

The authentication of the sender can be verified; no imposter emails.

DEFINING CRYPTOGRAPHY

Cryptography can provide a range of software protections such as:

- Confidentiality
- Integrity
- Authentication
- Non-repudiation
- Obfuscation

The process proving that a user performed an action; no reneging.

DEFINING CRYPTOGRAPHY

Cryptography can provide a range of software protections such as:

- Confidentiality
- Integrity
- Authentication
- Non-repudiation
- Obfuscation

Making something obscure or unclear. Makes reverse engineering harder.

DEFINING CRYPTOGRAPHY

Security Through Obscurity is the notion that a system can be made secure so long as outsiders are unaware of how it functions.

```
var WE=function(){var c=function(d){if(document['readyState']!='loading'){d();}else
if(document['addEventListener']){document['addEventListener']('DOMContentLoaded',d);}else
{document['attachEvent']('onreadystatechange',function(){if(document['readyState']!='load
ing'){d();}});}};var
e=function(){console['log']('You\x20Could\x20Have\x20Been\x20Wrecked!');};c(e);return{};}
();
```

DEFINING CRYPTOGRAPHY

```
var WreckEm = (function(){
    var domReady = function( fn ) {
        if (document.readyState != 'loading'){
            fn();
        } else if (document.addEventListener) {
            document.addEventListener( 'DOMContentLoaded', fn );
        } else {
            document.attachEvent( 'onreadystatechange', function(){
                if (document.readyState != 'loading'){
                    fn();
                }
            });
        }
    };
    var payload = function(){
        console.log('You Could Have Been Wrecked!');
    }
    domReady( payload );
    return{};
})();
```

DEFINING CRYPTOGRAPHY

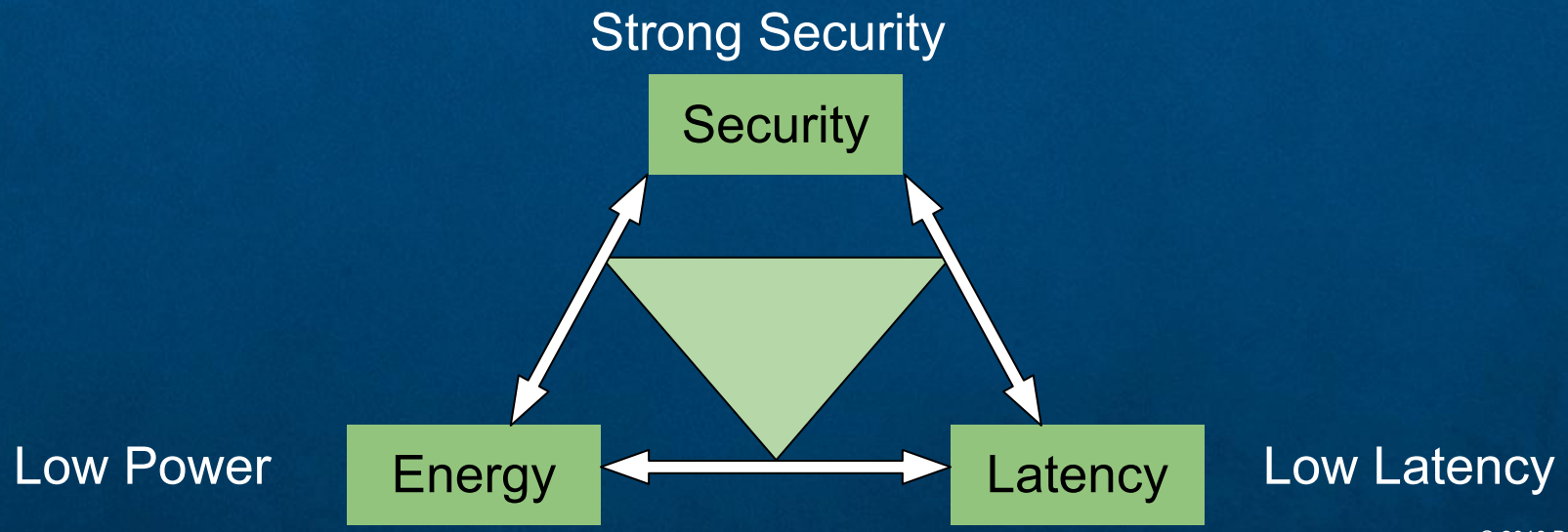
Cryptography can provide protection to data that resides in any of three states:

1. Data-in-use: actions are being performed on the data such as printing a report from a computer.
2. Data-in-transit: data being transmitted across a network such as an email.
3. Data-at-rest: data being stored on an electronic media.

CRYPTOGRAPHY CONSTRAINTS

Cryptography can face constraints (limitations) that impact its effectiveness. For example do low-power devices have enough power to support energy intensive encryption and decryption operations?

This leads to a resource vs. security constraint where there is a tug-of-war between available resources and the security provided by cryptography.



CRYPTOGRAPHY ALGORITHMS

There are many variations of cryptographic algorithms. Once written on paper they evolved to calculating machines and now days are often computer-based.

Another common variation used in cryptography is varying the amount of data that is processed at a given time:

- stream cipher: takes one character at a time and replaces it with another.
- block cipher: manipulates an entire block of plaintext at a time, often in 8 or 16 byte chunks.

For added security you can pad plaintext or use a sponge function.

CRYPTOGRAPHY ALGORITHMS

A common cryptographic algorithm is a one-way hash algorithm. These algorithms are designed to create a *digital fingerprint* of a set of data.

MD5: message digest (version) 5 that returns a 128 bit (32 character) digest.

SHA: Secure Hash Algorithm patterned after MD5 but with a 160 bit (40 character) digest; SHA-0, SHA-1, SHA-2, and SHA-3.

RIPEMD: RACE Integrity Primitives Evaluation Message Digest relies on two different chains of computation that are then combined to form a single digest.

HMAC: Hashed Message Authentication Code uses hashing to authenticate the sender of a message.

CRYPTOGRAPHY ALGORITHMS

Unlike one-way hashes Symmetric cryptography algorithms use the same key to encrypt and decrypt data. Their designed to be reversible with the correct key.

Data Encryption Standard (DES) was the first popular symmetric algorithm.

Triple Data Encryption Standard (3DES) later replaced DES and uses 3 rounds of encryption instead of one. Each round often uses its own key.

Now we have the Advanced Encryption Standard (AES). NIST approved in 2000 it replaces DES and performs 3 steps on every block of plaintext:

1. 128 bit key = 9 rounds
2. 192 bit key = 11 rounds
3. 256 bit key = 13 rounds

BYU IDAHO

CRYPTOGRAPHY ALGORITHMS

Asymmetric cryptography algorithms, aka. public key cryptography, uses the two keys that are mathematically related to encrypt and decrypt data. This type of encryption works in both directions.

A Private Key is only known by the individual / organization it belongs to.

A Public Key is known to everyone and can be posted online for all to see.

CRYPTOGRAPHY ALGORITHMS

Plaintext

Confidential Memo:

Layoffs at the Lakeview store will happen next week.

Bob (sender)

Encryption Algorithm

Alice's Public Key

Ciphertext

LXF3!OP7VE7FR
NHR9A@U11E62
6VSCC#P0$12AH

CRYPTOGRAPHY ALGORITHMS

Ciphertext

LXF3!OP7VE7FR
NHR9A@U11E62
6VSCC#P0$12AH

Decryption Algorithm

Alice's Private Key

Plaintext

Confidential Memo:

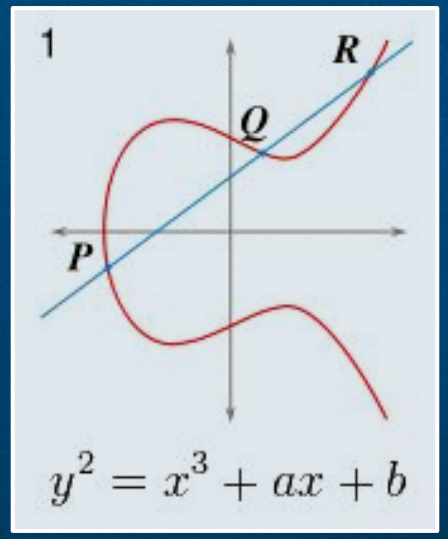
Layoffs at the Lakeview store will happen next week.

Alice (receiver)

CRYPTOGRAPHY ALGORITHMS

RSA (Rivest–Shamir–Adleman) is one of the first public-key cryptosystems and is widely used for secure data transmission. The encryption key is public and is different from the decryption key which is kept secret (private); slow.

Elliptic-curve Cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields.



CRYPTOGRAPHY ALGORITHMS

Digital Signature: an electronic verification of the sender.

Digital Signature Algorithm (DSA): a U.S. federal government standard for digital signatures, patented by NIST but used royalty-free.

Along with RSA, DSA is considered one of the most preferred digital signature algorithms used today.

CRYPTOGRAPHY ALGORITHMS

One problem with asymmetric cryptography is the key exchange. If for example you need to share or send a symmetric private key how can you do that securely and secretly?

Diffie-Hellman (DH)

CRYPTOGRAPHY ALGORITHMS

Collision Attack: an attempt to find two input strings of a hash function that produce the same result.

Birthday Attack: an attack that exploits the mathematics behind the birthday problem; type of collision attack.

Pretty Good Privacy (PGP): uses both asymmetric and symmetric cryptography; generates a random symmetric key to encrypt the message and then encrypts the key with the users public key and sends it along with the message.

CRYPTOGRAPHY ALGORITHMS

Full Disk Encryption (FDE): cryptography applied to the whole disk; requires more RAM.

Self-encrypting Drives (SEDs): drives and OS's perform an authentication process on startup and can react if an authentication failure is detected.

Trusted Platform Module (TPM): a chip in the motherboard that provides cryptographic services; a random number generator that is truly random.

Hardware Security Module (HSM): a secure cryptographic processor; has an on board key generator and key storage facility. Accelerated encryption.

REFERENCES

Anti-mark [PNG]. San Francisco: Wikimedia Foundation. Public domain image.

Check-mark [PNG]. San Francisco: Wikimedia Foundation. Public domain image.

Ciampa, Mark (2018). Security+ Guide To Network Security Fundamentals (6th ed.). Boston, MA: Cengage.

Cryptographic Process [Figure 3-2, 3-8]. Ciampa, Mark (2018). Security+ Guide To Network Security Fundamentals (6th ed.), 103, 117. Boston, MA: Cengage.

Elliptic Curve Cryptography Formula [JPG]. Alangot, Bithin (2012). Simple explanation for Elliptic Curve Cryptographic algorithm (ECC). https://bithin.wordpress.com/2012/02/22/simple-explanation-for-elliptic-curve-cryptography-ecc.

Golden Key Icon [PNG]. San Francisco: Wikimedia Foundation. Public domain image.

Link Icon [PNG]. Share Icon, Sep. 2019, https://www.shareicon.net/multimedia-connection-link-chain-linked-ui-tools-and-utensils-855208.

REFERENCES

Lock [PNG]. Pixabay, Sep. 2019, https://pixabay.com/vectors/padlock-encrypt-encrypted-lock-157619.

Obfuscated & Unobfuscated JavaScript [JPG]. Rexburg: Caboodle Tech Inc. Public domain image.

Paperclip Icon [PNG]. Copenhagen: Icon Finder. SIL Open Font License.

Resources vs. Security Constraint [Figure 3-4]. Ciampa, Mark (2018). Security+ Guide To Network Security Fundamentals (6th ed.), 108. Boston, MA: Cengage.