IT 489: IT Capstone Project—Spring 2016

Prof. Thomas Narock, Ph.D.

Assistant Professor of Management Science

Info Tech & Management Science, Marymount University,

Arlington, Virginia

Topic:

[DRAFT]

Is the government sanctioned level of encryption sufficient in keeping U.S. citizens and corporations safe from digital threats?

Date: March 4, 2016.

The case of Apple vs. FBI has turned the general public's attention to what encryption is and how it is handled by the government. The case being referred to pertains to the request from the government to ask the tech giant to unlock the iPhone used by the San Bernardino's gunman (Bergen). The mass shooting on December 2, 2015 at the Inland Regional Center in San Bernardino, California by a married couple (Syed Rizwan Farook and Tashkent Malik) left a total of 14 people killed and 22 were seriously injured (Rogers/Grummet). The issue at hand was access to the iPhone 5C used by the gunman which may have contained valuable information that may shed some light into the events preceding the shooting or the possibility of the existence of a third accomplice. The events in San Bernardino, California created an atmosphere of speculation about the function of the U.S. government levels of encryption being used to keep Americans safe from digital threats and acts of terrorism (Misener).

It is obvious that scrutiny of the concept of encryption at this moment is fueled by this case, and it has produced a catalyst to investigate how encryption works and why is it that encryption has become so important to keep our digital data, and by extension, our nation safe and secure. The case of the San Bernardino shooters is not the only case of government intervention nor is this the new state of affair when it comes to anti-terrorism in world history. Currently the government is dealing with 12 more cases for which they demand Apple unlock encrypted phones (Daily News). The earliest known case of encryption: over two-thousand years ago, Roman Emperor Julius Caesar created a cipher system that he employed between him and his commanders in the field. The Caesar's cipher is known as the earliest and simplest cipher language so far. Encryption is believed to be used by our Founding Fathers of the United States during the 17th Century. James Madison, Thomas Jefferson, George Washington, John Adams and John Jay were all prominent users of encryptions (Eff.org).

What is encryption?

The CompTIA Security + Guide to Network Security Fundamentals' textbook defines encryption as (P. 186/4th paragraph) the process of changing ciphertext into plaintext (Glossary/p.210). In simpler terms is "changing the original text into a secret message using cryptography." (CompTIA+, p. 186). Cryptography, on the other hand, is the science of transforming information into a secure form so that unauthorized persons cannot access it (CompTIA, p. 186). (See glossary)

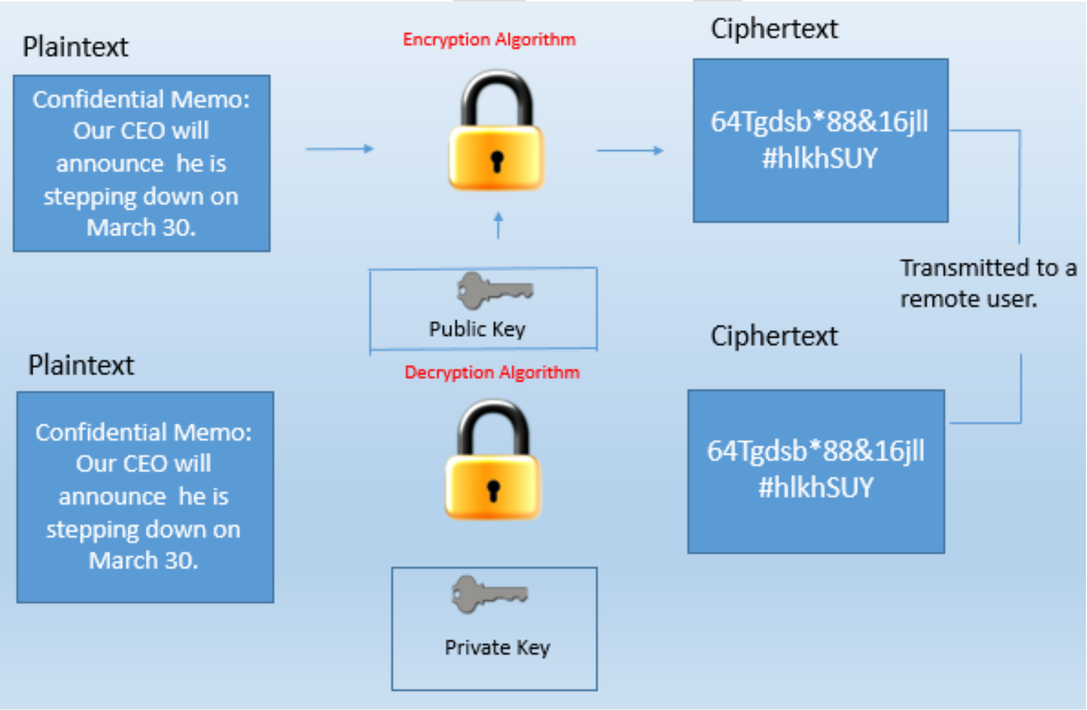

Plaintext
Confidential Memo: Our CEO will announce he is stepping down on March 30.
Encryption Algorithm
Ciphertext
64Tgdsb*88&16jll #hlkhSUY
Public Key
Transmitted to a remote user.
Plaintext
Decryption Algorithm
Ciphertext
Confidential Memo: Our CEO will announce he is stepping down on March 30.
64Tgdsb*88&16jll #hlkhSUY
Private Key

Figure 1 The Cryptographic process (CompTIA, Security + Guide to Network Security Fundamentals, p 187)

This process is also known as a digital signature. In order to sign a document as illustrated on the figure above, a digital certificate is needed. The digital certificate normally contains the following items: owner's name or alias, owner's public key, name of the issuer, digital signature of the issuer, serial number of the digital certificate, and an expiration date of the public key. (P. 231, CompTIA)

Digital Certificates:

One of the common applications of cryptography is digital certificates. Digital certificates are a technology used to associate user's identity to public key that has been "digitally signed" by a trusted third party. (IT 355/ Corporate Cybersecurity: Project Report: Digital Certificates--ongoing) Third party verifies owner and that public key belongs to that owner. An individual wishing to send an encrypted message applies for a digital certificate from a Certificate Authority. (CA) The CA issues an encrypted digital certificate containing the applicant's public key and a variety of other identification information. The CA makes its own public key readily available through print publicity or perhaps on the Internet. (Webopedia)

There are three types of digital certificates:

1. Personal Digital Certificates (Class 1)
   - For (individual) personal use.
   - Typically, it would need some form of user's name and email address in order to receive the certification.
2. Server Digital Certificate (Class 2)
   - Issued from a web server to a client
   - Ensures the authenticity of the web server.
   - Ensures the authenticity of the cryptographic connection to the web server.
3. Software Publisher Digital Certificates (Class 3)
   - Are provided by software publishers.
   - Goal is verifying their programs are secure and tamper-free programs

Government and Encryption

Consider the simple ways we use every day to protect our digital data: A User ID, a password, and an anti-virus program for our electronic devices. Or the use of USB sticks, SD cards, disks and back-up drives. But according to experts on this matter (Schneier/TED TALK), these are vulnerable to attack. In order to reinforce the initially vulnerable tech detection devices and firewalls, this may result in a higher price. It would involve the hiring of highly trained professionals and pricey maintenance contracts that comes with it. Regardless of all of these concerns, the most-effective way to protect data is to use encryption as the best option here. Sounds easy, right? In reality, this case has ramifications that not only the government, but citizens like you and me have started to analyze in a microscopic way. Whose phone is it: mine, Apple's, or the government? Considering these, then what levels of protection is the government considering to solve cases like this one?

Even when the perception of the term "encryption" is getting softer and less intimidating for Americans, still there is a perception that for them to be able to protect their personal privacy, it is a lot easier by abstaining from answering certain questions that are not relevant, or simply just offering misleading information. In an effort to attract Mozilla, the maker of Firefox has started a campaign (Encrypt) to help the public to understand encryption (CBC News). This was done under The Mozilla Foundation, which is a non-profit organization that exists to support and collectively lead the open source Mozilla project. (www.mozilla.org). Starting on February 21, 2016, it will consist of a series of short presentations in the forms of short videos, articles, and activities as a way to obtain the public's attention and involvement in understanding encryption. Since the word encryption sounds intimidating, the first video released was aimed at explaining encryption from a non-technical point. The main focus of the video was to explain to the general public in non-technical ways what encryption can do for people: protect their privacy.

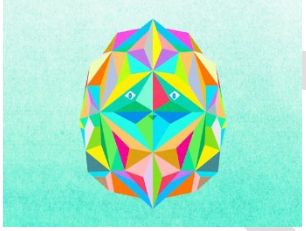
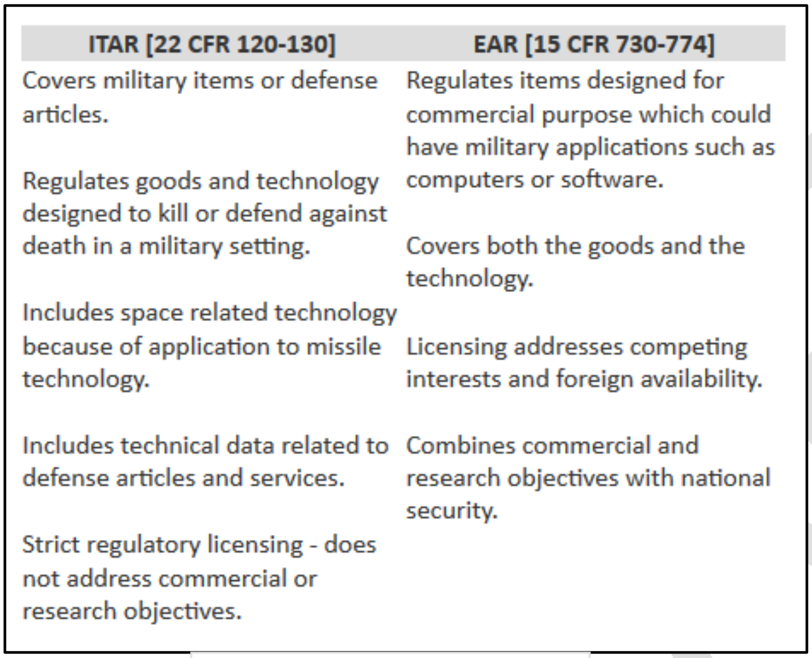


Figure 2: Mozilla Advocacy: Meet Encryption.

Save Crypto is an online petition asking President Obama "to come public on backdoors which allow certain companies to design systems to design their systems to give it special access to our data. Experts agree that backdoors of any kind would make all of our communications more vulnerable." (Save Crypto)

ITAR and EAR Compliances



ITAR [22 CFR 120-130]	EAR [15 CFR 730-774]
Covers military items or defense articles.	Regulates items designed for commercial purpose which could have military applications such as computers or software.
Regulates goods and technology designed to kill or defend against death in a military setting.	Covers both the goods and the technology.
Includes space related technology because of application to missile technology.	Licensing addresses competing interests and foreign availability.
Includes technical data related to defense articles and services.	Combines commercial and research objectives with national security.
Strict regulatory licensing - does not address commercial or research objectives.	

Figure 3:ITAR and EAR Compliances

The government exercises control of the use of encryption technology with two regulations: the ITAR and EAR compliances. The International Traffic in Arms Regulation (ITAR) is an export control regulation under the U.S. State department/Directorate of Defense Trade Controls, designed to help ensure that defense related technology does not get into the wrong hands. By ITAR standards “The U.S. Government views the sale, export, and re-transfer of defense articles and defense services as an integral part of safeguarding U.S. national security and furthering U.S. foreign policy objectives. Authorizations to transfer defense articles and provide defense services, if applied judiciously, can help meet the legitimate needs of friendly countries, deter aggression, foster regional stability. (PM.DDTC.STATE). Not only are there regulations on how to get authorized this type of encryption, the Export Administration Regulations, EAR, under the Department of Commerce is responsible to regulate the export of “dual-use” items, which include goods and related technology. That includes technical data and technical assistance as well. These two regulations were the result of the frequency of security breaches and terrorist attacks spanning the last 10 years. Pursuing any effort to ensure the privacy and security of our *private* communications is as important now as ever before. The roles and specifications of each one of the government's regulations are described on the following table:

Why is the government getting into the business of regulating technology as a product? In information technology, a product is something (for example, a software application) that is created and then made available to customers, usually with a distinct name or order number. (TechTarget). As technology continues to permeate every aspect of our lives, technology trade continues to become a big business. While the technology industry encourages the public to buy products and third party services over the Internet using credit card numbers, a large amount of personal information is being exposed to hackers (Grossman-& CNET). On September 29, President Bill Clinton released the first annual report to Congress of the Trade Promotion Coordinating Committee (TPCC), representing a substantial step toward producing results in the first of these approaches.

1. Encryption and the First Amendment

The **First Amendment** (**Amendment** I) to the United States Constitution prohibits the making of any law respecting an establishment of religion, impeding the free exercise of religion, abridging the freedom of speech, infringing on the freedom of the press, interfering with the right to peaceably assemble or prohibiting the petitioning for a governmental redress of grievances. It was adopted on December 15, 1791, as one of the ten amendments that constitute the Bill of Rights.

Berstein vs U.S., was the legal case involving (Northern District in California, 1995) Daniel J. Bernstein, a student from California, who challenged the restrictions on the export of cryptography from the United States.

2. Encryption and the Fourth Amendment

The Fourth Amendment guarantees the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things.

It seems like the Fourth Amendment protects the privacy rights on the physical world, but appears not to sufficient to protect the rights for privacy of what the cyberspace holds, This is a very challenging position for the law enforcement world. The cases of Riley v. California *and* United States v. Wurie, which both involved the search without a warrant; Riley, in California, had a smart phone, Wurie, in Boston had a flip phone. The judge in the Wurie's case did not side with him, and the judge in the Riley's case sided with him.

3. Encryption and the Fifth Amendment

The Fifth Amendment of the U.S. Constitution provides that, "No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a grand jury, except in cases arising in the land or naval forces, or in the militia, when in actual service in time of war or public danger; nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation."

Four court cases and the Fifth Amendment:

1. Commonwealth v. Gelfgatt (2012)

By a 5-2 decision, the Massachusetts Supreme Judicial Court (MSJC) ruled on June 25, 2014 that a criminal suspect can be ordered to decrypt his seized computer. The case involves a Massachusetts attorney named Leon Gelfgatt, who was allegedly involved in mortgage fraud. Prosecutors claimed that in 2009, Gelfgatt made over $13 million as a result of faking mortgage documents to sham companies. He was arrested in December 2009, and state troopers executed search warrants on his home and his vehicle, seizing four computers encrypted with "DriveCrypt Plus" software. (ARS TECHNICA/2014)

2. U.S. v. Feldman (2013)

An example of a ruling affirming that decryption is not a privilege. Jeffrey Feldman was accused of possession of child pornography in the state of Wisconsin in August 2013 (Eastern District of

Wisconsin.) The U.S. government's investigators try to force him to decrypt his computer's drives in order to abstract possible evidence in order to proceed with the case. The case took a different turn when the government's officials successfully cracked Feldman's password, therefore their petition before the court was dismissed. The case received a lot of public attention then because the judge initially decided that it was not permissible to allow the investigators' warrant to force Feldman to decrypt his hard drives. Then he overturned his own decision citing that the FBI agents "could not convinced him that couldn't establish to his satisfaction that Feldman controlled the computer." (Policeone)

3. In U.S. v. Doe (2012)

This was a case at the Eleventh Circuit (Northern District in Florida) presided by Hon..Gerald Bard Tjoflat who issued the first published appellate decision in the United States, in federal or state court, by holding that decryption is a privileged testimonial act. (Policeone/Brocklyn).

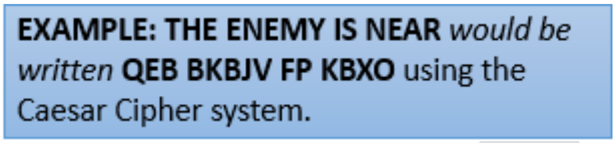
4. In U.S. v. Friscou (2012)

In U.S. v. Friscou (2012): Ramona Friscou was accused by the U. S. Government in a small-case mortgage scam in Colorado in 2012. (CNET) The computer she used was encrypted and she refused to turn over the computer's password to federal investigators. Friscosu's lawyer argued that turning over the computer's password would violate the rights she has under ***the Fifth Amendment*** that no one shall be compelled in any criminal case to be a witness against himself." The judge who presided over the case ordered Ms. Fricosu to provide the prosecutors an encrypted version of the hard drive. She was forced to provide the contents of her hard drive, but not the password to the laptop (Politics and Policy).

Understanding Mothern Encryption Techniques

The activity of encrypting, decrypting, and encoding is not something new on the modern history books. Roman Emperor Julius Caesar used to send secret messages to his commanders it when he was in the field. For example, The Caesar Cipher shifts the alphabet forward three places to create a new alphabet for sending secret messages. (NSA)

For example, the standard alphabet in our modern times looks like this: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z. Caesar Alphabet may have looked like this: X Y Z a B C D E F G H I J K L M N O P Q R S T U V W



EXAMPLE: THE ENEMY IS NEAR *would be written* **QEB BKBJV FP KBXO** using the Caesar Cipher system.