# Transcript: IT Podcast - Ep 108 - C836 Lesson 5 - with Arthur Moore and Jessica Galterio

*The following transcript is a verbatim account of the video or audio file accompanying this transcript.*

Speaker # 1: Arthur Moore

WGU's IT audio series. Flexible, portable, profound.

Hey, this is Arthur with WGU. I'm one of the course instructors for C836 Fundamentals of Information Security, and this is Chapter 5. Let's go ahead and jump into it. Just as a reminder, this series is there to supplement the reading material, not meant to replace the reading material. Also, this particular chapter is very acronym heavy, so it is advice that students take their own notes while going through it.

Let's get to it. It's highly recommended that you don't schedule the first assessment until all materials that have been covered. Take the pre-assessment, review lessons 1 through 12, pay close attention to Chapters 1 through 6, complete lessons 1 through 12 flashcards, pay close attention to Chapters 1 through 6, and complete lessons 1 through 12 quizzes and tests, and learn mode, paying close attention to Chapters 1 through 6.

What is cryptography? Cryptography is the study of cryptographic algorithms. These algorithms convert plain text, original message into ciphertext, the encrypted new message. Some algorithms work in both directions, allowing for these ciphertexts to return to your original plain text form, while others act as an integrity check, only allowing a one-way function. Crypto analysis is the breaking and finding of weaknesses in a given algorithm.

Cryptography is not new with information technology, cryptography is littered throughout history. One of the most ancient forms of it was by the Greeks and the Romans tattooing messages on the heads of their messenger and allowing the hairs to grow. I wonder if the poor messenger had any say whether or not his head was going to have a permanent tattoo. The next comes the Caesar cipher, which is based on trans positioning and shifting letters, plaintext message by a certain number of places, historically three, and to decrypt it, you would just shift it back in the opposite direction. Now, based on our level of understanding today, that does not seem very complex, but you have to understand during this time period in Rome with Caesar, most of the general population didn't know how to read. If you have somebody that could have read and then transpose and shift the message, it became nearly unbreakable until you had somebody else on the other end. Rot 13 uses the same metrics, same mechanism as the Caesar cipher, but moves each letter 13 places forward and to decrypt that you would just move it 13 places back.

Here are some little more modern cryptographic machines. We're not back in antiquity, now we're talking about the founding fathers. Thomas Jefferson created a purely mechanical cryptographic machine that was composed of 36 disk with a round edge on each disk to arrange the letters and numbers in a different order, and it was composed of 36 disk, one disk for each letter of the alphabet and zero through nine.

In order to decrypt the message on the other end, with a Jefferson disk, you would have to have the disketts arranged in the same order as the message was when it was encrypted. The German Enigma. Now we're looking at World War II. The German Enigma was developed in 1932, similar to that of the Jefferson disc, but with electro rotors and wheels.

It is still the same concept. When you have to the Enigma machines, and need to communicate, they have to be configured in the same way in order for the message to get across successfully.

Kerckhoff's principle says that security through obscurity is not the way to deal with the enemy, but to allow the algorithm to be known, and then to keep the key hidden itself. So the algorithm can be known to a world, it's the key itself that only needs to be kept secret.

Here are some modern cryptographic tools. Symmetric key cryptography, also known as private-key cryptography, uses a single key for both encryption and decryption. Asymmetric cryptography, also known as public key cryptography, uses a public key and a private key. The public key is used to encrypt, whereas the private key is used to decrypt.

The public key is shared with everybody, whereas the private key is only kept by the user. I want to point out symmetric key encryption, saying key, it says that it is also known as private key. Now, asymmetric cryptography is known as public key, two keys, but asymmetric cryptography has a private key. The private key is not known to anybody but the user themselves.

I just wanted to point that out. Hash functions are the third leg of the cryptographic tree, and it's what you might call keyless cryptography, because it's a one-way function. You put your message in, you get a fixed length hash out, and then you use that hash and you compare it again against the hash of the original message, and it's an integrity check. It's not a confidentiality item, it's an integrity check. Digital certificates allow us to sign the message, enable to detection of changes in the message content. Again, digital signatures are another integrity check, and it goes along with non-repudiation, making sure that the party that say they cannot deny that it was sent. Certificates are a link to a public key.

Certificates are most popularly known through the PKI, Public Key Infrastructure, dealing with CAs, RAs, and CRL list. A CA is a certificate authority, a RA is a registration authority, and a CRL is a certificate revocation list.

Symmetric cryptography, we've already explained it is having a private key. One key on both ends to let encrypt and decrypt. Symmetric key cryptography uses two types of ciphers, block ciphers and stream ciphers. Block ciphers, where it takes a certain amount of data as it goes through and encrypts it. This is why it's called block, because it actually takes a block of the data, where stream ciphers are going the plaintext message one bit at a time. The majority of the encryption algorithms that are used are block ciphers.

Here are some symmetric key algorithms. There's block cipher 56-bit key is deprecated. Triple D which is this encrypted three blocks times over with a different key, again, is deprecated. The majority of what's used today is AES and I would go as far as the say AES-256 would more than likely be the standard of what's used today.

Down below are some different block ciphers including Twofish cipher, Blowfish casts five our C6 and idea.

Asymmetric cryptography is also known as Public-key cryptography, and it utilizes two keys. Asymmetric two keys, a public key, private key. Public key can be known by anybody, whereas the private key is only known by the user. The main advantage of this is you can just have your key out in public and you don't have to worry about out-of-band transmission to get your message across.

Anybody can have your public key. They can encrypt the message with your public key and only you can decrypt it with your private key. Some asymmetric algorithms, RSA, ECC and PGP. Hash functions, like I said it represent the third leg of the cryptographic algorithms.

It's also called keyless cryptography. Hashes cannot be used to discover the contents of the original message. Again, it's a one way function. It goes in. It's an integrity check. It does not come out. Some algorithms are MD5 shot 2, shot 3, MD2, MD4, and RACE.

Digital signatures allow us to sign the message in order to enable detection of changes. Again, this is that integrity check that we're talking about. You want to make sure that the message was signed by the person that said they signed it. It makes it for non-repudiation.

Certificates and public key cryptography. Certificates are created to link a public key to a particular individual, often as a form of electronic identification for that particular person. A certificate is typically formed by taking a public key and identifying information such as a name, address, and having them sign by a certificate authority. The CA is a trusted entity, well known as like Verisign.

A CA is only a small part of the PKI infrastructure. PKI we also deal with the concept of certificate revocation, which is just like an exploration. Or for example, if the key gets lost, you want to go ahead and put the key for this is the private key. The public key is known to everybody. If the private key is discovered, you want to go ahead and make sure that that key pair, the public and private key pair are on that revocation list. They are not used anymore. Protecting data in motion, in rest and at use. These are the three states of data. When we talk about data, it is flowing, it's in use, I'm sorry. When it's flowing or when it's on the wire, it's in motion.

When it's sitting on a hard drive somewhere, be it a server, PC or a flash drive. It's in rest and it's in use when we're actively using it, processing it, creating, deleting, modifying.

To protect data at rest, you need to make sure that you encrypt data at rest and have very good physical security items around it. For example, laptops. They are been too many times in the news where because of a laptop being lost or stolen, that the hard drive wasn't encrypted. The bad actor was able to get to the social security numbers or whatever the case might have been on that particular device. Whenever we are dealing with data at rest, we got to have good encryption and good physical security. Make sure you have your laptop locks, make sure you have your two factor authentication, and make sure that the hard drive is encrypted. Data in motion is when data is traveling across the wire or cross the network. Protecting data in transit would be, again encryption, but we would use different encryption methods to do that, such as SSL, TLS, HTTP, VPNs, ISC, IPSec, which is a part of VPNs. There are different types of VPNs, which is the IPSec VPN and the SSL VPN.

Protecting data in use. Now, unfortunately, we can't encrypt data while it's in use because of the overhead that the encryption algorithm would take to encrypt and decrypt the data every time in order for it to be used.

The best way to go about protecting data while it's in use. It's educating the users on safe information security practices. Because we're limited in our ability to actually protect it while it's in use. But if we educate our users, or the ones that are processing, modifying, and changing the data. We will be able to protect it while it's in active use. This brings us to a close and thank you very much for joining me. Have a nice day.

Again, I appreciate you stopping by and listening to this audio series on C836, fundamentals of information security. With this, I would challenge you to contact your course instructors if you're having any issues within the course and apply these concepts to your daily lives and they will flow a lot easier. Thank you very much, and have a nice day.

Schedule time with your course instructor to explore more deeply. WGU, a new kind of you.