Top 30 Cryptographer Interview Questions and Answers for 2018

Introduction

What exactly is Cryptography? How can one exactly deploy this? For what purposes is it exactly used for? How can use it be used secure the confidential information and data of an organization? How can Cryptography be used to secure the lines of network communications between a remote worker the corporate servers?

These are all questions that a well-trained Cryptographer can answer. They are well versed in all aspects of this amazing part of Cyber security, with everything from its deployment to how it can best be used to meet the Security requirements of any organization.

In this article, we examine the top thirty questions that can be asked to an experienced Cryptographer, ranging from what it is all about to its commercial applications. These types of questions can be broken into down into Level 2 Questions, Level 3 Questions, and Level 4 Questions. These questions can also be used in an interview situation in those instances in which a business or a corporation wishes to hire a Cryptographer, either on a full time or contract basis.

The Level 2 Questions

In this grouping of questions, some of the fundamental questions behind Cryptography are asked, focusing upon:

- What it is all about;
- It's originations;
- It's goals and importance today;
- Message scrambling and descrambling;
- Ciphertexts;
- The Caesar and other related ciphers.

1) ***What is Cryptography***?

   Cryptography is a specialized area of Cyber security, but it has a broad array of applications, that we will examine later. Generally speaking it can be defined as follows:

   "Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents. In addition, cryptography also covers the obfuscation of information in images using techniques such as microdots or merging." (SOURCE: 1).

   In other words, is the science of scrambling a message at the point of origination, and it is descrambled at the point of destination into a decipherable format. During its transmission across a network medium, the message remains in a garbled format, so that if it were to be intercepted by a malicious third party, the content would be rendered useless. But, this process of scrambling and descrambling does not apply to just words, it can also be used to convert an image into a garbled state as well, according to the definition provided.

2) What exactly is encryption and decryption?

In terms of cryptography, the terms of scrambling and descrambling have much more specific terms associated with them. Respectively, scrambling and descrambling are also known as "encryption" and "decryption". So, for instance, the written message of "I LOVE YOU", when it is scrambled by the sending party becomes what is known as the "encrypted message", meaning that the written message has been disguised in such a manner that it would be totally meaningless, or in the terms of cryptography, it would be what is known as "undecipherable".

Also, encryption can also be further defined and described as "conversion of information from a readable state to apparent nonsense". (SOURCE: 2). Now, when the receiving party receives this encrypted written message, it must be descrambled into an understandable and comprehensible state of context. This process of descrambling is also known as "decryption".

3) What is a plaintext, or cleartext?

The decrypted message, when it is returned back into its plain or original state of context which is comprehensible and decipherable is also known as the "cleartext" or the "plaintext".

4) What is the ciphertext?

When the decrypted message is once again encrypted into a state of context which is totally incomprehensible and undecipherable, this is known as the "ciphertext". So, to illustrate all of this, with the previous example, when the sending party creates the written message of "I LOVE YOU", this is the plaintext or the cleartext.

Once this message is encrypted into the format of "UYO I VEOL", and while it is in transit, it becomes known as the ciphertext. Then, once the receiving party gets this ciphertext and then decrypts it into a comprehensible and understandable form of "I LOVE YOU", this message then becomes the plaintext or the cleartext, yet once again.

5) How does the encryption process actually take place?

This is a question in which we will have more specific answers for later on. But generally speaking, in its simplest form, the text or the written message is encrypted via a special mathematical formula. This formula is specifically known as the "encryption algorithm". Because the ciphertext is now encrypted by this special mathematical algorithm, it would be rendered useless to a third party with malicious intent, because of its totally garbled nature.

As the receiving party receives this ciphertext, it remains in its garbled format, until is it is descrambled. To do this, a "key" is used, which is only known by the sending party and the receiving party. In terms of cryptography, this key is also known as the "cipher", and it is usually a short string of characters, which is needed to break the ciphertext.

6) What are the originations of Cryptography?

It has its roots all the way back to 1900 BC. In Egypt, various hieroglyphic symbols were used to mask the identity of various tombs, with the best example of that being of the tomb that belonged to nobleman Khnumhotep II.

7) What is the Caesar Cipher?

With the Caesar methodology, each letter of the text or the written message is substituted with another letter of the alphabet which is sequenced by so many spaces, or letters later in the alphabet. This is probably the simplest form of encryption, because each letter in plain text message is literally substituted by another letter, thus forming the ciphertext. This methodology (which was developed by Julius Caesar) is probably the most cited type of algorithm in academic literature.

8) What is the goal of Cryptography?

Although the main purpose is to make content and images into an undecipherable format, the main goal of Cryptography is to ensure the Confidentiality, Integrity, and Availability of any Information Technology system. In other words, the content and images must remain private between the sending and the receiving parties; while they are in transit across the Internet assurances must be provided that they will remain intact and not altered in any way; and they must be content and images must be available at any time that they are requested.

9) Are there any other ciphers that are available other than the Caesar Cipher?

Yes, there are. As Cryptography has evolved over time, so has the degree of sophistication of these other ciphers, which include the following:

- Monoalphabetic ciphers;
- Polyalphabetic ciphers;
- Transpositions/Grills;
- Other various coding systems;
- Voice related scramblers (which can be found on wireless devices, such as Smartphones);
- Steganography.

10) Just how important is the field of Cryptography?

Cryptography is going to be play a very huge role today in Cyber security. For example, it will be vital to encrypt all kinds and types of information and data, especially as it relates to a business or corporation and their customers. We are seeing many instances where very sensitive information and data is being leaked to outside third parties (whether it is accidental or intentional). Also, as wireless communications are starting proliferate in terms of both adoption and usage, there will be a very strong need to ensure that they remain safe and secure.

The Level 3 Questions

This grouping of questions, intermediate level technical questions are asked to the Cryptographer candidate, focusing upon the following:

- Private Key and Public Systems;
- The traditional Security threats to cryptographic systems;
- Various cipher techniques (Polyalphabetic Encryption; Block Ciphers; Cipher Block Chaining);
- The disadvantages of Symmetric Key Cryptography;
- How a Key Distribution Center is used;
- The mathematical algorithms associated Symmetric Key Cryptography;
- Hashing Functions.

1) What is the difference between a Private Key and a Public Key?

As it was eluded to earlier, one of the main purposes of Cryptography is to scramble and forms of content and images into an undecipherable state. You might be wondering at this point how this is all exactly done. Well, it primarily involves the use of what is known as a key. The most traditional that has been used over time is that of the private key. With this particular key, the sending party can encrypt the plain text key, and from there, the content or image will be sent in its garbled state across the network medium to the receiving party. Once they receive it, the same private key is then used to decrypt the content or the image back into a decipherable state. However, since the same key is used, it is very important that both the sending and the receiving parties keep this key secret. If not, it could fall into the hands of a malicious third party, thus ciphertext vulnerable to being hijacked. Because of this security weakness, the public key was thus created. The sending party uses this particular key to encrypt the content or image, but it is important to note that the receiving party is not aware of this public key. Rather, they still use the private key to decrypt the ciphertext.

2) What are Symmetric and Asymmetric key systems?

A symmetric key system uses only the private key, and the asymmetric key system makes use of both the public key and the private key. The latter used primarily in what is known as a "Public Key Infrastructure", or "PKI" for short. It will be discussed in more detail later on.

3) What kinds of threats are there for a Cryptographic system?

There are three traditional types of attacks, and they are as follows:

- Ciphertext-only attack: With this type of attack, only the cipher text is known to the attacker. But, if this particular individual is well trained in statistics, then he or she can use various statistical techniques, to break the ciphertext back into the plaintext;

- Known-plaintext attack: This occurs when the hacker knows some aspect of either the letter pairings, thus, they can consequently crack the ciphertext back into the plaintext;

- Chosen-plaintext attack: With this type of attack, the hacker can intercept the natural plaintext message which is being transmitted across the network medium, and from this, reverse engineer it back into its ciphertext form, in an attempt to figure out the specific encryption scheme.

  But it is important to keep in mind that as the Cyber threat landscape has changed dramatically, there are many newer variants which have come out based on the above attack scenarios.

4) What is Polyalphabetic Encryption?

This was listed as a specific type of cipher earlier. With this, multiple types of Caesar ciphers are used, but these ciphers are used in a specific sequence, which repeats once again when the overall cipher has reached its logical end the first time, in order to finish the completion of the encryption of the plaintext message.

This means that the wrap around technique is also prevalent in this type of scenario. Let us illustrate this example once again with "I LOVE YOU". Building upon the example used previously, suppose that two types of Caesar ciphers are being utilized, such as where k=1, and k=2 ("k" once again denotes the actual Caesar cipher, or the sequential spacing of the number of letters later in the alphabet).

The overall cipher algorithm utilized is C1 (k=1), C2 (k=2) where C denotes the Caesar key. So, with the example of using "I LOVE YOU", using the polyalphabetic algorithm, it would be encrypted as "J ORYF BPX". To understand this further, the first letter in the plaintext is C1, so I am represented as J, the second letter of the plaintext is C2, so C is represented as O, and so on.

The logical end of the cipher algorithm is C2, so once again, it reaches the logical end of its first iteration, it then wraps around once again as C1 (k=1), C2 (k=2) the second time around, then the third time around, until the plaintext message has been fully encrypted.

So, in our illustration of "I LOVE YOU", there were a total of three iterations of C1 (k=1), C2 (k=2), in order to fully encrypt the plaintext.

5) What is a Block Cipher?

With this method of transposition, the plaintext message is then encrypted into its scrambled format. Let us illustrate this again with our example used before, but this time, let us assume a block of three characters, mathematically represented as 3 bits, or where k=3.

Plaintext:	I LOVE YOU
Plaintext Block:	ILO VEY OUX
Ciphertext Block:	OLI YEV XUO
Ciphertext:	OLIYEVXUO

Note that an extra character as added at the end, which is the letter "X". This was added so that a complete plaintext block can be formed. As a rule of thumb, if the total number of characters in the plaintext is not divisible by the block size permutation (in this instance, where k=3), then it can be safely assumed that extra characters will be needed to the plaintext in order for the last block of plaintext to be considered as complete. This is known as "padding". It should be noted that the most widely used block is where k=8 bits long.

As we can see, even with the simple example from up above, block ciphers are a very powerful tool for symmetric key cryptographic systems. After all, it goes through a set number of iterations of scrambling, in order to come up with a rather well protected ciphertext.

6) What is Cipher Block Chaining?

The Initialization Vectors are part of a much larger process known as "Cipher Block Chaining", or "CBC" for short. Within this methodology, multiple loops of encryption are created, in order to totally further scramble the ciphertext. Here is the how the process works:

(1) The Initialization Vector is created first;
(2) Through a mathematical process known as XOR (which stands for exclusive OR, and is used quite frequently to determine if the bits of two strings of data match or not), the first created Initialization Vector is XOR'd, with the first block of ciphertext data;
(3) The first chunk of data which has been XOR'd is further broken down by another layer of encryption;
(4) This process is then continued until all of the blocks of ciphertext have been XOR'd and enveloped with another layer of encryption.

Thus, this is how Cipher Block Chaining gets its title. For instance, steps 1-4 as detailed up above creates the first loop or chain, the second loop or chain is then next initiated, and so on, until the ciphertext has been fully analyzed and encrypted by this methodology.

7) What are the disadvantages of Symmetric Key Cryptography?

Symmetric Key Cryptography suffer from three major vulnerabilities, which are as follows:

1) Key Distribution;
2) Key Storage and Recovery;
3) Open Systems.

As previously mentioned, symmetric cryptography requires the sharing of secret keys between the two parties (sending and receiving), which further requires the implicit trust that this key will not be shared with any other outside third party. The only way that any type of secrecy can be achieved in this regard would be to establish some sort of trusted channel. An option here would be the use of a so called designated "controller". But, this carries third party risks as well.

With regards to the second vulnerability, since there will be many more lines of communication between the sending and the receiving parties, the need to implement more controllers

becomes totally unrealistic as well as infeasible. Thus, the distribution of the private keys can become a virtual nightmare.

Finally, with the third vulnerability, private or symmetric cryptography works best only when it is used in a very closed or "sterile" environment, where there are at best only just a few (or even just a handful) of sending and receiving parties. In other words, given the threat landscape today, it would be completely unrealistic to implement a symmetric cryptography system in an open environment.

8) How is a Key Distribution Center (KDC) used?

The Key Distribution Center, consists of a database of all of the end users at the place of business or corporation, and their respective passwords, as well other trusted servers and computers along the network.

If an end user wishes to communicate with another end user on a different computer system, the sending party enters their password into the KDC, using a specialized software called "Kerberos". When the password is received by the KDC, the Kerberos then uses a special mathematical algorithm which adds the receiving party's information, and converts it over to a cryptographic key.

Once this encrypted key has been established, the KDC then sets up and establishes other keys for the encryption of the communication session between the sending and the receiving party. These other keys are also referred to as the "tickets". These tickets have a time expiration associated with them, so the ticket will actually expire at a predetermined point in time, in order to prevent unauthorized use, and it would also be rendered useless, if it is stolen, hijacked, or intercepted by a third party.

9) What are the mathematical algorithms used in Symmetric Cryptography?

They are as follows:

1) The Needham-Schroder algorithm:

   This algorithm was specifically designed for KDC systems, in order to deal with sending and receiving parties who appear to be offline.

2) The Digital Encryption Standard algorithm (DES):

   This mathematical algorithm was developed in 1975, and by 1981, it became the de facto algorithm for symmetric cryptography systems. This is a powerful algorithm, as it puts the ciphertext through sixteen iterations in order to ensure full encryption.

3) The Triple Digit Encryption Standard algorithm (3DES):

   This mathematical algorithm was developed as an upgrade to the previous DES algorithm just described. The primary difference between the two of them is that 3DES puts the

ciphertext through three times as many more iterations than the DES algorithm.

4) The International Data Encryption Algorithm (IDEA):

This is a newer mathematical algorithm than 3DES, and is constantly shifting the letters of the ciphertext message around constantly, until is decrypted by the receiving party. it does not consume as much processor power as the DES algorithms do.

5) The Advanced Encryption Standard algorithm (AES):

This is the latest symmetric cryptography algorithm, and was developed in 2000.

10) What is the Hashing Function?

It is a one-way mathematical function, meaning, it can be encrypted, but it cannot be decrypted. Its primary purpose is not to encrypt the ciphertext, rather its primary purpose is to prove that the message in the ciphertext has not changed in any way, shape or form. This is also referred to as "message integrity".

The Level 4 Questions

This category of questions, advanced level technical questions are asked to the Cryptographer candidate, focusing upon the following:

- What Asymmetric Key Cryptography is;
- Some of the major differences between Asymmetric Key Cryptography and Symmetric Key Cryptography;
- The advantages and disadvantages to using Asymmetric Cryptography;
- The typical mathematical algorithms that are used in Asymmetric Cryptography;
- The Public Key Infrastructure (PKI) and how it works;
- The Certificate Authority;
- How the LDAP used in a Public Key Infrastructure;
- The Security vulnerabilities of Hashing Functions.

1) *What Is Asymmetric Key Cryptography?*

In the most simplistic terms, Asymmetric Cryptography can be likened to that of a safety box at a local bank. In this example, normally, there are two set of keys which are used. One key is the is the one which the back gives to you. This can be referred to as the public key, because it is used over and over again. The second key is the private key which the bank keeps in their possession at all times, and only the bank personnel know where it is kept.

The world of asymmetric cryptography is just like this example, but of course, it is much more complex than this in practice. To start off with, typically, in asymmetric cryptography, let us refer to the public key as "pk", and the private key as "sk".

So, to represent both of these keys together, it would be mathematically demonstrated as (pk, sk). It is then the sending party which uses the public key (pk) to encrypt the message they wish to send to the receiving party, which then uses the private key (sk) to decrypt the ciphertext from the sending party.

2) What are the key differences between Asymmetric & Symmetric Cryptography?

First, with Symmetric Cryptography, the complete 100% secrecy of the key must be assured. Whereas, as it has been just described, Asymmetric Cryptography requires only half of the secrecy, namely that of the private key (sk).

Second, Symmetric Cryptography utilizes the same secret key for the encryption and decryption of the ciphertext, but with Asymmetric Cryptography, two different keys (namely the public and the private keys) are both used for the encryption and the decryption of the ciphertext.

In other words, in Asymmetric Cryptography, the roles of the sender and the receiver are not interchangeable with one another like symmetric cryptography. This means that with Asymmetric Cryptography, the communication is only one way. As discussed, because of this, multiple senders can send their ciphertext to just one receiver, but in Symmetric Cryptography, only one sending party can communicate with just one receiving party.

3) What are the Disadvantages of Asymmetric Cryptography?

Despite the advantages that Asymmetric Cryptography has, it does possess one very, serious disadvantage: When compared to symmetric cryptography, it is two to three times much slower than symmetric cryptography. This is primarily because of the multiple parties which are involved, and the multiple keys which are involved also.

Thus, it can take an enormous amount of processing power, and it can be a serious drain to server power and system resources.

There are two specific cases in which an Asymmetric Cryptographic system can be hacked. First, is the situation if the hacker replaces a public key of their own (mathematically represented as pk'), while the ciphertext is in transit between the sending and the receiving parties, and the receiving party decrypts that ciphertext with the malicious public key (pk').

The second situation arises when the hacker can change the mathematical value of the public key, or change it while it is in transmission between the sending and the receiving parties.

4) What are the Mathematical Algorithms used in Asymmetric Cryptography?

There are three of them that are primarily used, and they are as follows:

(1) The RSA Algorithm;

(2) The Diffie-Hellman Algorithm;
(3) The Elliptical Wave Theory Algorithm.

In terms of the RSA Algorithm, this is probably the most famous and widely used Asymmetric Cryptography algorithm. The RSA Algorithm originates from the RSA Data Security Corporation, and is named after the inventors whom created it, which are: Ron Rivest, Adi Shamir, and Leonard Adelman.

The RSA Algorithm uses the power of prime numbers to create both the public key and the private key. But, using such large keys to encrypt such large amounts of data is totally infeasible, from the standpoint of the processing power and central server resources. Instead ironically, the encryption is done Symmetric Algorithms.

Once the receiving party obtains their ciphertext from the sending party, then the private key generated by the Symmetric Cryptography Algorithm is decrypted, then the public key which was generated by Asymmetric Cryptography can then be subsequently used to decrypt the rest of the ciphertext.

In terms of the Diffie Hellman Asymmetric Algorithm, it is named after its inventors as well, whom are Whit Diffie and Martin Hellman. It is also known as the DH algorithm for short as well. But interestingly enough, this algorithm is not used for the encryption of the ciphertext, rather the main concern of it is to address the problem for finding a solution of the issue of sending a key over a secure channel.

Here is a summary of how it works, on a very simple level:

(1) The receiving party as usual has the public key and the private key that they have generated, but this time, they both are created by the DH Algorithm;
(2) The sending party receives the public generated by the receiving party and uses this DH Algorithm to generate another set of public keys and private keys, but on a temporary basis;
(3) The sending party now takes this newly created temporary private key and the public key sent by the receiving party to generate a random, secret number-this becomes known as the “session key”;
(4) The sending party uses this newly established session key to encrypt the ciphertext message, and sends this forward to the receiving party, with the public key that they have temporarily generated;
(5) When the receiving party finally receives the ciphertext from the sending party, the session key can now be derived mathematically;
(6) Once the above step has been completed, the receiving party can now decrypt the rest of the ciphertext.

Finally, with Elliptical Wave Theory, it is a much newer type of Asymmetric mathematical algorithm. It can be used to encrypt very large amounts of data, and its main advantage is that it is very quick, and does not require a lot of server overhead or processing time. As its name implies, Elliptical Wave Theory first starts with a parabolic curve drawn on a normal x, y coordinate of any given Cartesian plane.

After the first series of X and Y coordinates are plotted, various lines are then drawn through the image of the curve, and this process continues until many more curves are created and their corresponding, intersecting lines are also created.

Once this process has been completed, the plotted X and Y coordinates of each of the intersected lines and parabolic curves are then extracted. Once this extraction has been completed, then all of the hundreds of X and Y coordinates are then added together in order to create the public and the private key.

But, the trick to decrypting a ciphertext message encrypted by Elliptical Wave Theory is that the receiving party has to know the shape of the original elliptical curve, and all of the X and Y coordinates of the lines where they intersect with the various curves, and the actual starting point at which the addition of the X and Y coordinates first started.

5) What is the Public Key Infrastructure (PKI)?

Since the public key has become so important in the encryption and the decryption of the ciphertext messages between the sending and receiving parties, and given the nature of the of its public role in the overall communication process, great pains and extensive research have been taken to create an infrastructure which would make the process of creating and sending of the public keys as well as the private keys much more secure and robust.

In fact, this infrastructure is a very sophisticated form of Asymmetric Cryptography, and it is known as the "Public Key Infrastructure", or "PKI" for short. The basic premise of PKI is to help create, organize, store, distribute, and maintain the public keys. But, in this infrastructure, both the private and public keys are referred to as "Digital Signatures", and they are not created by the sending and receiving parties, rather they created by a separate entity known as the "Certificate Authority".

6) What are the specific components of the Public Key Infrastructure (PKI)?

The PKI consists of the following components:

(1) The Certificate Authority, also known as the CA: This is the outside third party whom issues the digital certificates;
(2) The Digital Certificate: As mentioned, this consists of both the private key and the public key, which are issued by the CA. This is also the entity that the end user would go to in case he or she needed to have a digital certificate verified. These digital certificates are typically kept in the local computer of the employee, or even the central server at the place of business or organization;
(3) The LDAP or X.500 Directories: These are the databases which collect and distribute the digital certificates from the CA;
(4) The Registration Authority, also known as the RA: If the place of business or organization is very large (such as a multinational corporation), this entity then usually handles and processes the

requests for the required digital certificates, and then transmits those requests to the CA to process and create the required digital certificates.

7) ***What are the technical specifications of the Certificate Authority?***

The Certificate Authority consists of the following technical specifications:

(1) The Digital Certificate Version Number: Typically, it is either version number 1, 2, or 3;
(2) The Serial Number: This is the unique ID number which separates and distinguishes a particular Digital Certificate from all of the others (this can be likened to each Digital Certificate having its own Social Security Number);
(3) The Signature Algorithm Identifier: This contains the information and data about the mathematical algorithm used by the Certificate Authority to issue the particular Digital Certificate;
(4) The Issuer Name: This is the actual name of the Certificate Authority which is issuing the Digital Certificate to the place of business or organization;
(5) The Validity Period: This contains both the activation and deactivation dates of the Digital Certificates, in other words, this is the lifetime of the Digital Certificate as determined by the Certificate Authority;
(6) The Public Key: This is created by the Certificate Authority;
(7) The Subject Distinguished Name: This is the name which specifies the Digital Certificate owner;
(8) The Subject Alternate Name Email: This specifies the Digital Certificate's owner Email address (this is where the actual Digital Certificates go to);
(9) The Subject Name URL: This is the Web Address of the place of business or organization to whom the Digital Certificates are issued to.

8) How does the Public Key Infrastructure (PKI) work?

At a macro level, this is how the Public Key Infrastructure (PKI) works:

(1) The request for the Digital Certificate is sent to the appropriate Certificate Authority (CA);
(2) After this request has been processed, the Digital Certificate is issued to the person whom is requesting it;
(3) The Digital Certificate then gets signed by confirming the actual identity of the person whom is requesting that particular Digital Certificate;
(4) The Digital Certificate can now be used to encrypt the plaintext into the ciphertext which is sent from the sending party to the receiving party.

The Registration Authority, (aka the "RA") is merely a subset of the CA. It is designed to help if it becomes overwhelmed with digital certificate request traffic.

However, the RA by itself does not grant any type or kind of digital certificates, nor does it confirm the identity of the person whom is requesting the digital certificate. Rather, its role is to

help process the requests until the processing queue at the CA becomes much more manageable.

The RA sends all of the digital certificate requests in one big batch, rather than one at a time. This is process is known as “chaining certificates”.

Finally, all digital certificate requests are processed by the RA are also associated with a chain of custody trail, for security auditing purposes. The RA can be viewed as a support vehicle for the CA, in which a mathematical, hierarchal relationship exists.

9) What is the LDAP Protocol & how is it used in a Public Key Infrastructure (PKI)?

The LDAP is an acronym which stands for “Lightweight Directory Access Protocol”. This is a database protocol which is used for the updating and searching of the directories which run over the TCP/IP network protocol (this is the network protocol which is primarily used by the PKI Infrastructure).

It is the job of the LDAP server of the Public Key Infrastructure to contain information and data as it relates to the digital certificates, the public and the private key storage locations, as well as the matching public and private key labels.

The Certificate Authority uses a combination of the end user name and the matching tags to specifically locate the digital certificates on the LDAP server. From that point onwards, it is the LDAP server which then checks to see if the requested digital certificate is valid or not, and it if it is valid, it then retrieves from its database a digital certificate which can then be sent to the end user.

Although all digital certificates which are issued have a finite lifespan when they are first issued, they can also be revoked for any reason at any time by the Public Key Infrastructure Administrator.

10) *What are the Security vulnerabilities of Hashing Functions?*

A major security vulnerability of using Hashes is that they can even be altered while it is end route. In other words, a Cyber attacker can intercept the ciphertext and its associated hash, alter both, and create a brand new ciphertext and a brand-new hash.

As a result, the receiving party is then fooled into believing that this new, altered ciphertext, and that the new altered hash is the original sent by the sending party, while the Cyber attacker keeps the actual ciphertext and hash which was generated the first time around.

To fix this, the ciphertext is combined with a “secret key” at the point of origination first, then the hash is created. As a result, this hash will then contain specific information and data about the secret itself. As a result, the receiving party can even be further ensured that the ciphertext they have received is the original one sent by the sending party.

This is so because even if the ciphertext, the hash, and the associated secret key were to be intercepted, there is very little that a hacker can do to alter the ciphertext and its associated hash, because they have to have the information and data about the secret key, which is of course something they will never gain access to.

Conclusions

Overall, this article has examined some of the major as well as more challenging aspects of Cryptography. A well-versed Cryptographer should be able to answer these, as well as well as the candidate whom is applying for a Cryptographer level position. In the case of the latter, a good candidate should be able to answer these questions to some degree of detail.

As a recruiter, it is imperative to put your Cryptographer candidate to the test, after all, it will be your organization that will be relying upon him or her in order to fortify the lines of Security at the endpoints an in the middle.

It is important to note that Cryptography is heavily dependent upon the usage of mathematics; therefore, the Cryptographer candidate or even one that is currently employed should have a solid background in this area as well.

As a candidate, if you really want that Cryptographer position and out beat your competition, reviewing this article in depth will help you to get that lucrative position. Also, to get that extra edge, you can review more Cryptography based Q and A's here.

Sources

1) https://usa.kaspersky.com/resource-center/definitions/what-is-cryptography
2) "Computer Networking: A Top Down Approach, Kurose, J.F. & Ross, K.W., Pearson Education Group, 2008 p. 683.
3) https://access.redhat.com/blogs/766093/posts/1976023
4) https://allabouttesting.org/cryptography-interview-questions/
5) http://www.inf.ufsc.br/~bosco.sobral/ensino/ine5680/material-cripto-seg/2014-1/Stallings/Stallings_Cryptography_and_Network_Security.pdf
6) http://www.ccs.neu.edu/home/noubir/Courses/CSU610/S06/cryptography.pdf
7) http://faculty.nps.edu/dedennin/publications/Denning-CryptographyDataSecurity.pdf
8) https://www.saylor.org/site/wp-content/uploads/2012/07/Public-key-infrastructure1.pdf
9) ftp://ftp.rsa.com/pub/pdfs/understanding_pki.pdf
10) https://handouts.secappdev.org/handouts/2011/Bart%20Preneel/preneel_cryptographic_algorithms_2011.pdf