ANALYSIS ON CRYPTOGRAPHY

FOR CYBER SECURITY

A glance of internet safety

Abstract

SHA, RSA and MD5 are working together protecting our privacy

Hui Zhao

101159615@georgebrown.ca

Index

Introduction of Cryptography

Cryptography or **cryptology** (from Ancient Greek: κρυπτός, romanized: *kryptós* "hidden, secret"; and γράφειν *graphein*, "to write", or -λογία *-logia*, "study", respectively[1]) is the practice and study of techniques for secure communication in the presence of third parties called adversaries. Cryptography prior to the modern age was effectively synonymous with *encryption*, the conversion of information from a readable state to apparent nonsense. Modern cryptography is heavily based on mathematical theory and computer science practice. [1]

Cryptography plays an important role in our modern daily life. It helps us to protect the credentials and sensitive information, such like, username and password we use to login Amazon.ca or the PIN we use to login our mobile bank. Without encryption, our private information will be easily intercepted by a third party due to the http protocol not encrypted. Without cryptography, the e-business will not be developed so well and give users less convenience like today.

---

[1] https://en.wikipedia.org/wiki/Cryptography

There are two flavours of encryption: symmetric crypto and public key crypto. Both of them have pros and cons.

The most famous public key crypto algorithm is RSA. It is named by using the initial letters of the surnames of the 3 MIT professors who publicly described their algorithm firstly in 1977. RSA algorithm based on the difficulty of prime factorization. [2] In other words, without the help of quantum computers, RSA is impossible to be cracked. The only downside is using quite a lot CPU process time which means it needs a lot of compute power to encrypt and decrypt. So, RSA is the best choice for public key change and not suitable for encrypting payload.

Unlike RSA, AES is a symmetric algorithm which is using less compute power. AES is widely supported by modern CPU both x86 and ARM instruction architecture. Morden CPU can do the AES process very quickly. So it is the perfect choice for encrypt/decrypt the payload.

MD5 and SHA are both symmetric algorithms, they are widely being implemented by checking the integrity of the file when downloaded from the internet. Also they are being used for AH(authenticate header)in Cisco VPN implementation.

All the algorithms above are widely used by modern internet security implementations in our daily life.

How does Cryptography help Integrity?

Cryptography can also be used to ensure the integrity (or accuracy) of information through the use of hashing algorithms and message digests.[3]

---

[2] https://en.wikipedia.org/wiki/RSA_(cryptosystem)

[3] https://www.oreilly.com/library/view/cissp-for-dummies/9781118417102/a2_13_9781118362396-ch08.html

Ideally, we can use RSA to encrypt all the data we transferred online because it is almost impossible to break. But in reality, RSA needs quite a lot of CPU resources which is the main reason it is hard to break. It's not practical using RSA to encrypt all the data for http protocol. For the majority, RSA is used for public key exchange and using AES for the payload in https protocol. And SHA is using CA to sign the signature to the RSA key pair. The SHA helps CA to keep the RSA key pair unchanged(integrity) and popular browsers such like: Chrome, Edge, Safari, Firefox have a built-in CA list. The unsafely http protocol is encrypted by RSA/AES into much safer protocol https which provides us safety to use our credit card on Amazon or check our bank balance on smartphone using mobile bank APP without worry about the leaking of any personal information including bank account and PIN or credit card information.

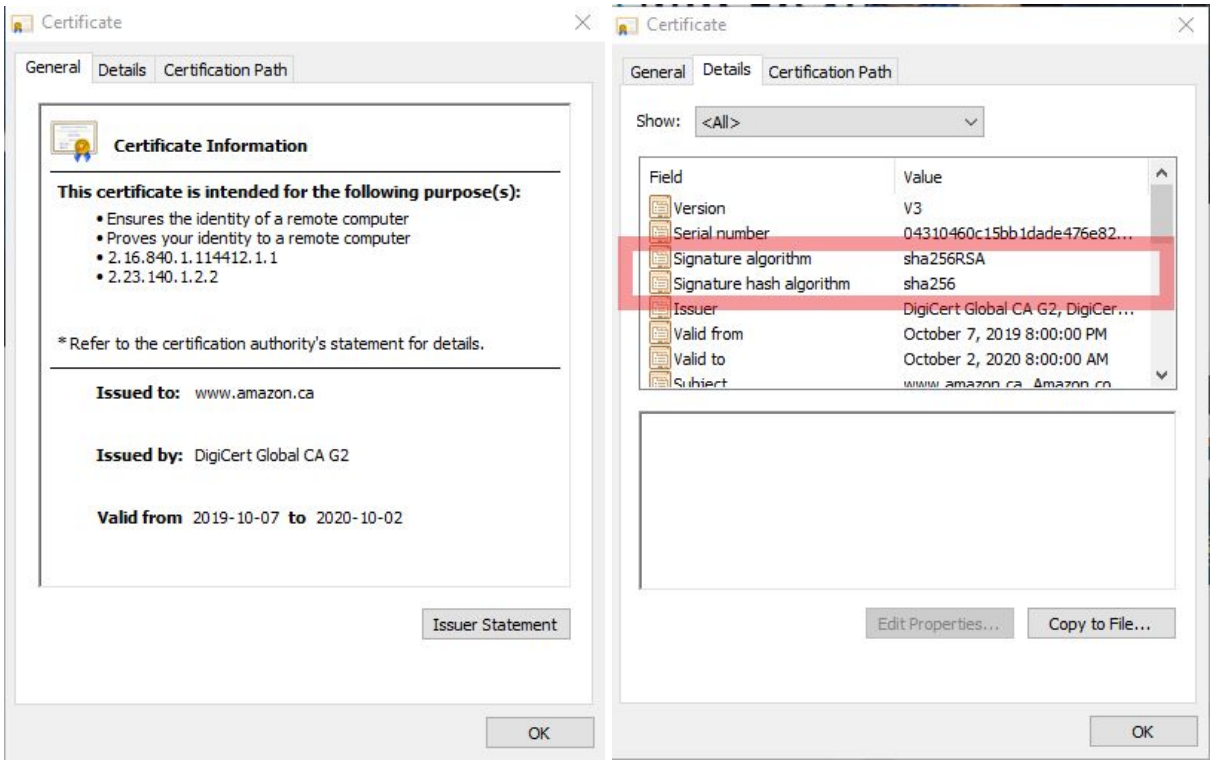

Fig 1-1 RSA public key of Amazon.ca is signed by DigiCert with 256 bits SHA

SHA guarantees the integrity of the RSA key pair which means the SHA will protect the modification to the RSA key from others except the owner.

For example, when I am using Chrome browsing amazon.ca, amazon has a public RSA key which is signed by DigiCert (Fig 1-1). Amazon.ca pays DigiCert who is one of many CAs, as exchange, DigiCert signs a signature to amazon's RSA key pair(public and private) to make sure the amazon's keys are trustworthy. The DigiCert plays as the third-party guarantee that all the information between me and Amazon.ca is encrypted and safely kept between Amazon and myself. In this case, Chrome has a built-in set of Root CA list, and DigiCert is trusted by one of them. Because the trustworthy can be inherited, the browser will consider DigiCert is trustworthy and show the SSL icon in the front of URL (fig 1-2). Otherwise, the browser will give a warning that we are visiting an insecure website. Amazon uses this signed RSA key pair to encrypt/decrypt the conversation between my browser and his server. (Fig 1-3)

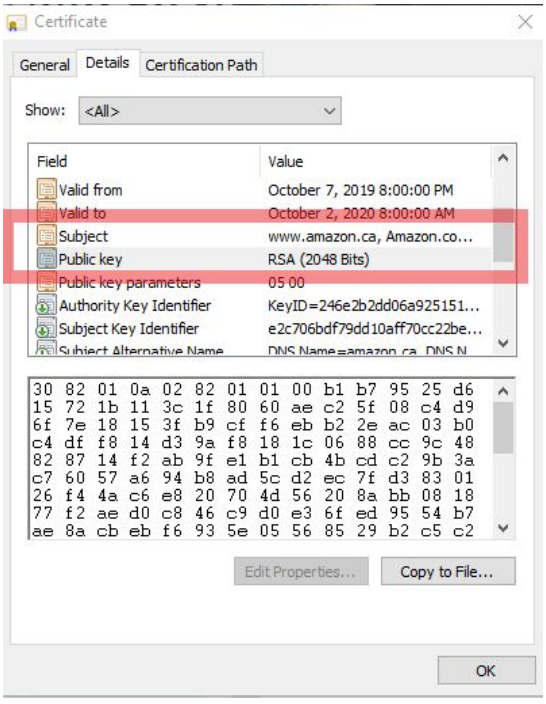

Fig 1-3 Amazon.ca is using 2048 bits RSA

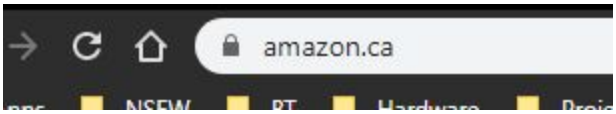

Fig 1-2 there is a lock icon in front of URL, it shows SSL enabled

Another example is MD5/SHA widely being used to verify the file you download from the internet is not corrupt. (Fig 1-4)

Sometimes the file you download from the internet will become corrupt. Using SHA and MD5 will help the user to check the integrity of the file itself. You can run the checksum tools, compare the original hash value and the hash value you get. If they are the same, means your file is untouched, the copy you get is identical to the original one.

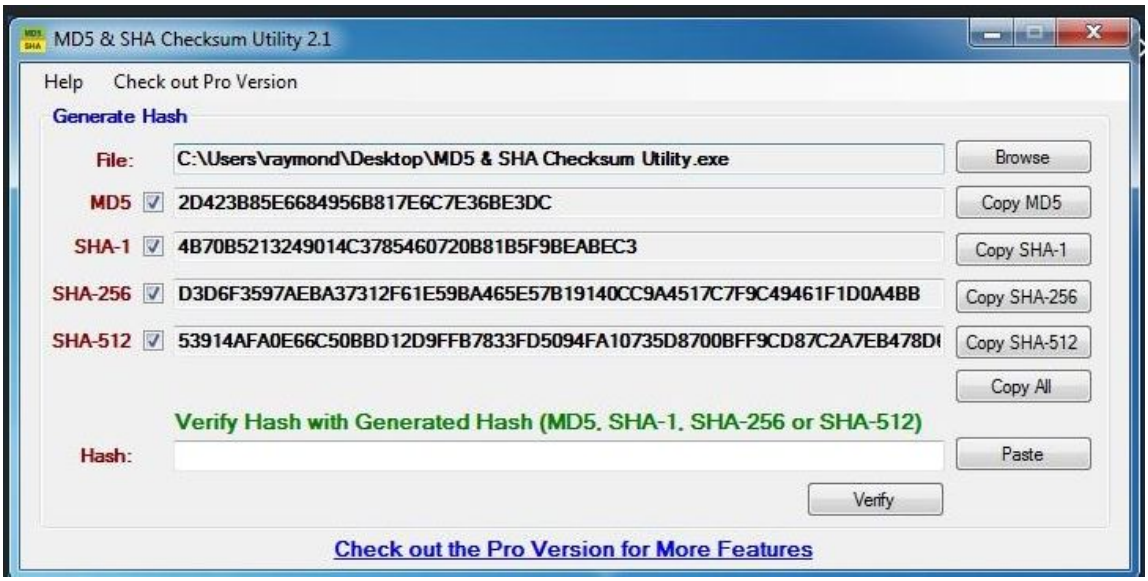

Fig 1-4 MD5 and SHA checksum tools

Above all, that's how cryptography helps the integrity of cyber security: CA signatures guarantee the RSA key pair is from the owner and is not changed by anyone else.

How does Cryptography help Authenticity?

In cryptography, a message authentication code (MAC), sometimes known as a tag, is a short piece of information used to authenticate a message—in other words, to confirm that the message came from the stated sender (its authenticity) and has not been changed. The MAC value protects both a message's data integrity as well as its authenticity, by allowing verifiers (who also possess the secret key) to detect any changes to the message content.[4]

As we see in the amazon example, SHA is being used for CA(DigiCert) sign the signature to the RSA key pair to ensure the RSA key pair is coming from the owner (amazon.ca), not anyone else. (Fig 1-1)

A test of cryptography helping authenticity is using certificates to enable SSL on the server side. If the certificate is installed on the server and has a different domain which is defined inside the certificate, the certificate will not work. The CA ensures the signature to RSA key pair issues to the authentic owner.

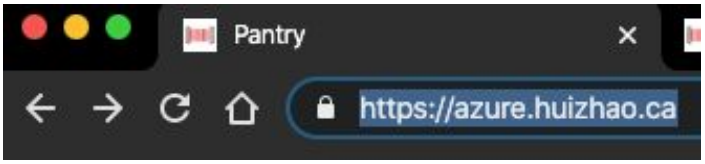

Fig 2-1 SSL enabled for azure.huizhao.ca

For example, I have a certificate signed by “Let's Encrypt” registered under my domain azure.huizhao.ca works and only works under that domain. (Fig 2-1) If I using azure1.huizhao.ca

[4] https://en.wikipedia.org/wiki/Message_authentication_code

to visit it, even it will be resolved into same ip address as azure.huizhao.ca , but the browser will not enabled SSL by default and give you a warning that the certification has issue. (Fig 2-2)

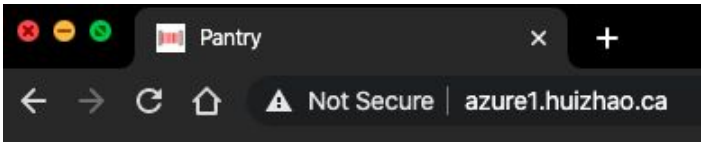

Fig 2-2 SSL disabled for azure1.huizhao.ca

This test confirmed that only the legit owner of the RSA key pairs can be used to build a https/ssl connection between server and client. My RAS keys for A domain can not be used for B domain. Thus, the RSA ensures the authentication of the data.

Another example is ESP(Encapsulating Security Payload) and AH(Authentication Header). They both use a symmetric algorithm (a pre-shared key) to authenticate the data origin(source of packet) and using MD5/SHA to ensure the payload(IP packet).

The AH protocol provides a mechanism for authentication only.[5]

AH(Authentication Header) is a member of the IPsec protocol suite. It provides authentication, data origin authentication and data integrity. Data integrity using a digest algorithm such as MD5 or SHA. Data origin authentication is ensured by a shared key to create message digest. Reply protection is covered by AH header. It authenticates the entire IP packets: IP and payloads, but some header can be altered legitimately during the transmission, such as TTL.

The ESP protocol provides data confidentiality (encryption) and authentication (data integrity, data origin authentication, and replay protection).[6]

[5] https://www.ibm.com/support/pages/what-difference-between-ah-and-esp-protocols-ipsec
[6] https://www.ibm.com/support/pages/what-difference-between-ah-and-esp-protocols-ipsec

ESP(Encapsulating Security Payload) provides functions like AH, but more flexible. It provides the free combination between authentication and confidentiality(payload encryption). It has different coverage when it does the authentication job, though it uses the same algorithm with AH. Unlike AH, ESP authentication only verifies the portion of the IP packet.

Above all, we can see the cryptography using RSA public key pair, MAC,AH and ESP for the implementation of the authentication of cyber security.

How does Cryptography help Confidentiality?

Cryptography protects the confidentiality (or secrecy) of information. Even when the transmission or storage medium has been compromised, the encrypted information is practically useless to unauthorized persons without the proper keys for decryption.[7]

The RSA algorithm is an asymmetric encryption algorithm, encrypting an input into an output that can then be decrypted (contrast a hash algorithm which can't be reversed). It uses a different key for encryption (the public one) than for decryption (the private one). This can therefore be used to receive encrypted messages from others - you can publish your public key, but only you with the private key can then decrypt the messages that have been encrypted with it.

Due to RSA using different keys to encrypt and decrypt, it is widely used for the counter measure of the notorious MITM(Man in the middle) attack which usually asymmetric encryption can not. The reason is obvious, MITM intercept all the data between victims including the symmetric key for encoding and decoding the data. Once the symmetric key is

---

[7] https://www.oreilly.com/library/view/cissp-for-dummies/9781118417102/a2_13_9781118362396-ch08.html

compromised, the data is not safe anymore. On the contrary, the RSA algorithm uses different keys to encrypt and decrypt the data. Even if the encoding(public) key is intercepted by a man in the middle, the data is still safe(until the private key is compromised).

By helping with the RSA algorithm, the data is not vulnerable from MITM attack, which means no third party can know what happened between the first and second party. Therefore, the confidentiality of data is preserved. For example, when I shop on amazon.ca, all data including username and password, credit card information are encrypted and safe. No third party including the man in the middle can know what happened between amazon.ca and me.

Another example is VPN, VPN can use both symmetry key and public key algorithm to conceal the traffic. The mechanism is the same as HTTPS/SSL. The data between peers is ciphered and no third party can understand what happened between the peers. VPN can avoid the MITM attack as well. Btw, the VPN was the first choice of Chinese netizens to get around the Great FireWall because of the conflict between the censorship of Chinese government and the warship for freedom of Chinese netizens.

The last one not the least is the famous Tor, AKA “Onion Routing”, its slogan is “Browse Privately,

Explore Freely”. Onion routing is implemented by encryption in the application layer of a communication protocol stack, nested like the layers of an onion. Tor encrypts the data, including the next node destination IP address, multiple times and sends it through a virtual circuit comprising successive, random-selection Tor relays. [8]

[8] https://en.wikipedia.org/wiki/Tor_(anonymity_network)

Due to Tor using encrypted next hop, nobody knows who is the next router. So nobody can trace the data. Even more, before the data reaches the destination, it will jump at least 3 anonymous hops. This strategy helps the data prevent the tracking of third parties. Nobody can find the data, so it keeps the confidentiality of the data.

Above all, The cryptography using RSA/SHA/MD5 algorithm to implement VPN/SSL protocol who help the confidentiality of cyber security.

Conclusion

The cryptograph uses all kinds of algorithms such as MD5, SHA, RSA, et al to implement the protocols such as HTTPS, SSL, AH and ESP etc. By following the standard of these protocols, the application can protect the integrity, authenticity and confidentiality of data, thus the cyber security.

Google just announced quantum supremacy last year. [9] It means 2048 bits RSA is not safe anymore. Will the fundamentals of modern cryptography be changed in the future? Will the RSA algorithm be obsolete in the future? The answer definitely is yes, the only question is how fast.

April 2020 Toronto

[9] https://www.nytimes.com/2019/10/23/technology/quantum-computing-google.html