Bogenberger - Damsell, O., Cleary E., Crowley, T., Kocik, D., McMorrow, R. (2020) Report on Cryptography, University of Limerick, unpublished

**Abstract:**

**Introduction**

**Early History**

Caesar Cypher first actual use of cryptography to hide messages.

"Caesar used it in order to   
if there was occasion for secrecy, he wrote in cyphers; that is, he used the alphabet in such a manner, that not a single word could be made out. The way to decipher those epistles was to substitute the fourth for the first letter, as d for a, and so for the other letters respectively." The Twelve Caesars 56.Gaius Suetonius Tranquillus. Translator:Alexander Thomson

Due to the Power and enemies he had aquired in Rome Caesar needed a good way to keep his messages secret.The Caesar is of course a simple form of cryptography but as it was close to the first use of cryptography it didnt need to be too complex, and the caesar cypher was also suprisingly used in modern computing in the ROT13 method as a low security way of hiding information. this method was used more to protect the viewer from potentially offensive language or information.Another interesting adaption of the Caesar Cypehr in history was the Vigenère cipher.

Vignere cipher first use of encryption key

**Cryptography and early computing**

Hebern rotor machine.

Enigma.and Bombe machine.

**Early modern history**

Ibm crypto group and Lucifer(D.E.S. Data Encryption Standard)

1997 NIST encryption (Advanced Encryption standard).

**Cryptography and modern computing**

//also discuss key terms, mention cryptography and encryption were synonymous

//Terms to mention: key(randomness),

**Symmetric cryptography (Secret key?)**

The formal definition of symmetric encryption is “an algorithmic tool that allows a pair of parties to communicate secret information over open communication media that are accessible to eavesdroppers.” (Theory of Cryptography Conference Corporate 2010) This is a classic model of encryption, where the both parties share a secret key. The key is assumed to be random, single-purpose and not dependant on the message. The security is ensured by the fact that encryption and decryption happen in safe environments and the adversary cannot intercept the key.

**Introduction(explanation)**

**Stream cipher**

**Common attacks**

**Public key cryptography**

**Introduction**

(Buchanan, William J. Cryptography, pg 144/ 155)

Public key encryption or asymmetric key encryption uses both a public and private key to secure a communication between two entities. The public key is shared and distributed while the private key is kept private and secure. The mathematics of the encryption make it really difficult to determine one key when given the other key because of how difficult it is to factor a value for its prime number factors, it is so difficult that it should take conventional computers thousands of years of computing time to decrypt. This is achieved using the following methods. **Integer factorization** (RSA method) **discrete logarithms** (ElGamal)and **elliptic curve relationships** (Elliptic Curve).

Public key encryption is often used for identity checking. It checks the identity of the entity by using its public key to decrypt a message that was encrypted using the entities private key. Since the two keys are mathematically linked then they can only be decrypted using the other so if it can be decrypted by the public key then it proves its identity.

It can also be used for protection of a symmetric key. This tends to be used in disc encryption where the symmetric key that is used to encrypt a file is protected with the public key of an entity so then the only key with access to the symmetric key is the private key.

Of course it’s most common use is to establish secure communications. When two entities want to communicate securely they simply exchange their public keys and use them to encrypt the data they want to send to the other. That way the only entity that can decrypt the message is its intended recipient who holds the private key.

The key is usually stored in an XML format or on a digital certificate which allows it to be stored processed and transmitted this is known as the (PKI) or the Public Key Infrastructure. Where key pairs are generated by trusted entities the private key is kept secret while the public key is distributed using the PKI. The most important part of the PKI is the keeping of the private key secret. If the private key loses its secrecy then the security and identity of the entity could be breached as well as the any encryption keys that are protected by the key pair.

## RSA

The public and private keys are generated from very large prime numbers as a value which is the product of another two large prime numbers that is extremely to factorize. The public key is then passed where it is used to encrypt data intended to be sent to the entity.

The most used and well known algorithm in RSA selects two large prime numbers that are usually around 256 bits in length *a* and *b* and are also to the order of 10100, these factors are then kept secret and you make the modulus N by multiplying them together. Then to make the second public key you choose another value *e* so that *e* and (*a* – 1) × (*b* - 1) are relatively prime as in they do not share a common factor bigger than 1 so GCD (*x, y*) = 1. The public key is then <*d, N*> and this makes a key that is at least 512 bits long.

The private key for decryption *d* is computed so that:

*d = e-1 mod [(a – 1) × (b - 1)]*

*Or*

*(d × e) mod [(a-1)(q-1)] = 1*

PHI is defined as *(p -1) × (b-1).* The encryption process to the *c* is *= me mod N,* and the message *m* is then decrypted with the formula *m = cd mod N.*

**EIGamal**

The keys are generated using a description of a cyclic group *G* of order *q* with the generator *g*. *e* is represents the unit element of *G*. A random integer *x* is then chosen from *{1,…, q - 1} h := gx.* The public key is made from the values *(G, q, g, h)* and *x* is kept as the private key.

The message is encrypted by mapping it to an element *m* of *G* with a reversible mapping function. You choose another random integer *y* from *{1, …, q -1}*. Compute the shared secret *s := hy* as well as *c1 := gy* and *c2 := hy c2 :m × s* and send the cipher text *(c1, c2)* to the intended recipient of the message.

*(c1, c2)* is decrypted with the private key *x* by computing *s := c1x* because *c1 := gy,* *c1x* *= gxy* = *hy* which is the same shared secret used. *s-1*, the inverse of *s* is then computed in the group *G*. You then compute *s-1* as *c1q-x* because of Laranges theorem which states *s × c = gxy × g(q - x)y = (gq)y = ey = e*. *m := c2 × s-1* is then computed producing the original message because *c2 = m×s* so *c2 × s-1 = (m×s) s-1* *= m×e = m*. the result *m* is then mapped onto the message

**Common attacks**

**Hash functions**

**Introduction**

**Message Authentication**

**SHA1,2,3,**

**MD5**

**Common attacks**

**Crypto cracking**

**Other technologies that rely on cryptography**

**Blockchain**

**VPN**

A VPN or Virtual Private Network.

**Short note on future of cryptography(quantum)**

**Conclusion**

**List of references**

# ***Cryptography and Public Key Infrastructure on the Internet (2006)***

# ***By Klaus Schmeh***

*Mjølsnes, S. F. et al. (2008) Public Key Infrastructure 5th European PKI Workshop: Theory and Practice, EuroPKI 2008 Trondheim, Norway, June 16-17, 2008, Proceedings . 1st ed. 2008. [Online]. Berlin, Heidelberg: Springer Berlin Heidelberg.*

**Bibliography**

Canetti R., Tauman Kalai, Y., Varia, M., and Wich, D. (<https://link-springer-com.proxy.lib.ul.ie/book/10.1007%2F978-3-642-11799-2>)

Theory of Cryptography Conference Corporate, A. (2010) *Theory of Cryptography 7th Theory of Cryptography Conference, TCC 2010, Zurich, Switzerland, February 9-11, 2010, Proceedings*,1st ed. 2010. ed., Berlin, Heidelberg:Springer Berlin Heidelberg.