An Introduction to Public-Key Cryptography

By:

Matthew Sutton

March 30th, 2017

Advanced Writing for IS&T

Table of Contents

For Final Copy: Table of Contents/List of Tables & Figures

Introduction

For over three-thousand years there was no viable key exchange method for establishing secure communications (Shelton, 2015). Humans were stuck using secret-key cryptosystems (symmetric cryptography) in which parties need a separate, secure channel for key exchange. The process of securely communicating keys over unsecured mediums was not thought up until the 1960s. Government Communications Headquarters (GCHQ) cryptographer, James H. Ellis, wrote a previously classified journal on the need for "*non-secret encryption"* (Barr, 2002, p. 243). "Non-secret encryption" is defined as the concept of having a cryptosystem where some functions of the encryption process are publicly-facing without leading to any compromise. Without knowing about the GCHQ classified journal, 1970s Stanford Researchers Whit Diffie, Ralph Merkle, and Martin Hellman ended up inventing the first *public-key cryptosystem* and, therefore, solved the key exchange problem (Odlyzko, 1994, p. 19). Humans have only been using public-key cryptography for approximately half a century as compared to secret-key's multi-millennia existence.

Essentially, *public-key cryptography* (asymmetric cryptography) is a cryptographic system for parties who wish to establish secure communications without the need to have had previously communicated a shared-secret. It has revolutionized Internet communications by enabling the concept of "non-secret encryption" where parties can engage in secure communication without previously exchanging keys. Additionally, key management for public-key cryptosystems requires significantly less overhead than secret-key cryptosystems. Each party enrolled in a public-key cryptosystem has an outward-facing public key and a confidential private key. Anyone can send confidential messages by encrypting their message content using a recipient's public key. Subsequently, an encrypted message can only be decrypted by the recipient's private key. Overall, public-key cryptography provides the following capabilities:

- ***Key-Exchange***
  "Thanks!" & "Thanks!"

- ***Authentication via Digital Signatures***
  "I am confirmed to be who I say I am."

- ***Sender Non-Repudiation***
  "I cannot refute that I sent that message."

- ***Message Authentication***
  "This message was not modified during transmission."

This report is organized in such a fashion that readers at different levels of cryptography knowledge can start at different points. For those who have little to no cryptography knowledge, start at Cryptography Fundamentals. For others who are familiar with cryptography, start at Secret-Key Cryptography (Symmetric Cryptography).

Cryptography Fundamentals

What is cryptography?

Cryptography is defined as "the science and art of designing and using methods of message concealment" (Barr, 2002, p. 2). It is considered an art due to the finesse required to develop reversible, yet complex, mathematical functions also known as *ciphers*. Typically, ciphers apply a *key* in the mathematical function where the key must be kept secret or a message can be decoded with ease. Fundamentally, cryptography takes readable data, called *plaintext*, and applies a cipher/secret key combo to create a new form of incomprehensible data called *ciphertext*.

What is a cryptosystem?

Entities using cryptography apply two processes, entitled *encryption* and *decryption*, to complete a *cryptosystem*. Encryption is defined as the process of encoding plaintext using a cipher to create ciphertext. Decryption is defined as the process of decoding ciphertext to reveal the original plaintext. Essentially, cryptosystems are a series of reversible mathematical functions used in conjunction to achieve *confidentiality*. Confidentiality is one of the prime objectives of information assurance. Confidentiality is defined as the confidence that there has been no unauthorized access to data. Fig. X. shows a basic illustration of a cryptosystem and visually applies the terms encryption and decryption.

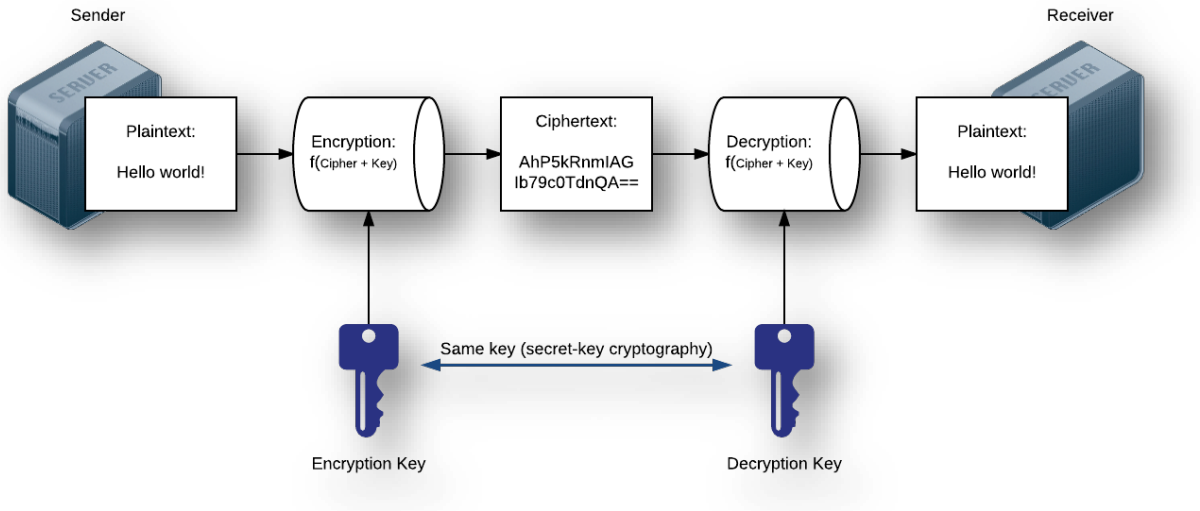


Fig. X. Illustration of a Cryptosystem Implementing Secret-Key Cryptography (AES 128-bit)

Why do we need cryptography?

“Human being[s] from ages ha[ve] two inherent needs – (a) to communicate and share information and (b) to communicate selectively. These two needs gave rise to the art of coding the messages in such a way that only the intended people could have access to the information. Unauthorized people could not extract any information, even if the scrambled messages fell in their hand.” ("Origin of Cryptography", n.d., para. 1)

Ideas: Here I plan to explain all the hops a typical message takes on the Internet. First, your message is routed through your ISP. A typical message then hops around ten-plus times over a few different networks as it travels across the world. Without encryption, at any of these points your data can be exposed. Additionally, there is always the threat of eavesdroppers on your network. Rogue access points are a real threat to secure networks. Individuals will snoop in and setup their own access point within a secure network. If your traffic is encrypted, you can be assured that your information is secure regardless of intruders or eavesdroppers.

Can I trust that cryptography will secure my data?

Kerckhoff's principle – one ought to design systems under the assumption that the enemy will gain full familiarity with them (Krebs, 2015, para. 10). I will also engage on the complexity behind encryption.

What are the different types of ciphers?

Substitution ciphers replace letters of the alphabet to encode the plaintext.

Plaintext	H	E	L	L	O	R	E	A	D	E	R
Encryption Substitution		E = X	L = Z	L = Z			E = X			E = X	
Ciphertext	H	X	Z	Z	O	R	X	A	D	X	R
Decryption Reverse Substitution	H	X = E	Z = L	Z = L	O	R	X = E	A	D	X =	R
Plaintext	H	E	L	L	O	R	E	A	D	E	R

Fig. X. A Simple Substitution Cipher of Letter L with Z and E with X

Monoalphabetic ciphers are substitution ciphers where the cipher alphabet is fixed through the entire encryption process. The Caesar Cipher was a monoalphabetic shift cipher used in 50 B.C. (Barr, 2002, p. 5). It applied a constant shift substitution of the alphabet.

Cipher Alphabet:

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Casear Cipher:

Plaintext	H (7)	E (4)	L (11)	L (11)	O (14)	R (17)	E (4)	A (0)	D (3)	E (4)	R (17)
Encryption Shift +5	+ 5	+ 5	+ 5	+ 5	+ 5	+ 5	+ 5	+ 5	+ 5	+ 5	+ 5
Ciphertext	M (12)	J (9)	Q (16)	Q (16)	T (19)	W (22)	J (9)	F (5)	I (8)	J (9)	W (22)
Decryption Shift -5	- 5	- 5	- 5	- 5	- 5	- 5	- 5	- 5	- 5	- 5	- 5
Plaintext	H (7)	E (4)	L (11)	L (11)	O (14)	R (17)	E (4)	A (0)	D (3)	E (4)	R (17)

Fig. X. Caesar Cipher with a Shift of 5

Polyalphabetic Ciphers are substitution cipher where the cipher alphabet is changed during the encryption process. The Caesar Cipher can once again be applied here, but this time a running key will be used. Instead of applying the same shift throughout, a polyalphabetic alphabet is created using a running key of 12345 in Fig. X.

Cipher Alphabet:

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Casear Cipher:

Plaintext	H (7)	E (4)	L (11)	L (11)	O (14)	R (17)	E (4)	A (0)	D (3)	E (4)	R (17)
Encryption Running Key	+ 1	+ 2	+ 3	+ 4	+ 5	+ 1	+ 2	+ 3	+ 4	+ 5	+ 1
Ciphertext	I (8)	G (6)	O (14)	P (15)	T (19)	S (18)	G (6)	D (3)	H (7)	J (9)	S (18)
Decryption Running Key	- 1	- 2	- 3	- 4	- 5	- 1	- 2	- 3	- 4	- 5	- 1
Plaintext	H (7)	E (4)	L (11)	L (11)	O (14)	R (17)	E (4)	A (0)	D (3)	E (4)	R (17)

Fig. X. Caesar Cipher with a Running Key Shift of 12345

A *transposition cipher* rearranges plaintext to create ciphertext.

Ideas: An example of a transposition cipher will go here. Specifically, columnar transposition.

Secret-Key Cryptography

Introduction

Secret-key cryptography is a form of cryptography where a same key is used for encrypting and decrypting.

History

"Secret-Key cryptography is the oldest form of encryption and has been used to safeguard communications for over three-thousand years" (Shelton, 2015). The first forms of cryptography belonged to the Ancient Egyptians. They would communicate by *hieroglyphs* where their language was only known to the scribes ("Origin of Cryptography", n.d., para. 6). Romans advanced cryptography from 400-500 B.C. by applying monoalphabetic shifts such as in the Caesar Cipher ("Origin of Cryptography", n.d., para. 7). It was not until 1553 century that polyalphabetic ciphers came to existence. The *Vigenere Cipher* applied a 26x26 grid where substitutions took place with cross-sectional lookups (see Fig. X.).

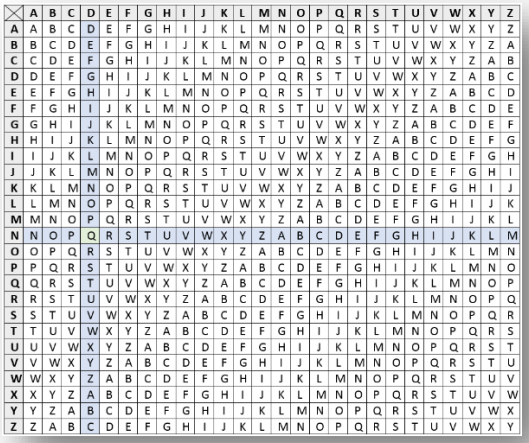
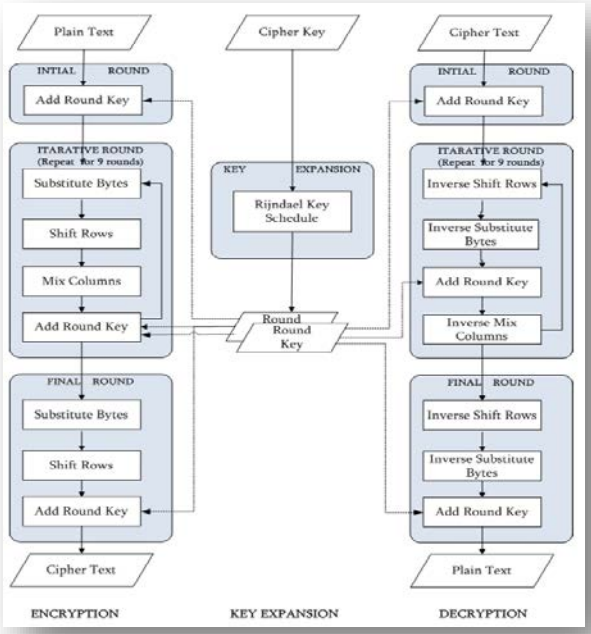


Fig. X. A Vigenere Lookup of Letter N by key D to Reveal Ciphertext Q (Hammond, 2015)

Ideas: I will discuss how World War 2 brought the Nazi Enigma Machine, one of the first forms of mechanical encipherment. Further, I will explore modern cryptography and leave off with the Advanced Encryption Standard (AES) block cipher. This will connect all the previous cipher information and explain the complexity of modern cryptography. I plan to use this image to visually explain the complexity today:



- ***Substitute Bytes*:** a non-linear substitution step where each byte is replaced with another byte according to a substitution table
- ***Shift Rows*:** a transposition step where each row of the state is shifted cyclically a certain number of steps.
- ***Mix Columns*:** a mixing operation which operates on the columns of the state, combining the four bytes in each column. Applies matrix math.
- ***Add Round Key*:** a bit wise exclusive OR operation is performed between each byte of the state and the round key which is generated from the cipher key using the Rijndael key schedule algorithm.

Fig. X. AES 128-bit Algorithm Diagram and Accompanying Definitions (Hasib & Haque, 2008, p. 506)

What are the pros of secret-key cryptography?

Symmetric cryptography is designed to quickly encrypt and decrypt large amounts of data. The previously mentioned AES cipher is built into modern day hardware. Intel processors have included AES instructions in their central processing unit (CPU) hardware since 2010 (Gueron, 2012, para. 1). This allows for "secure and high performance AES implementations" (Gueron, 2012, para. 5).

Modern forms of symmetric cryptography are exceptionally strong. Table X shows the possible number of keys for each AES key size form. It is theorized that the NSA cannot even directly brute force AES encryption. Top security expert, Bruce Schneier (2012), states:

"...[My guess is the NSA doesn't] have a cryptanalytic attack against the AES algorithm that allows them to recover a key from known or chosen ciphertext with a reasonable time and memory complexity."

Key Size	Possible Key Combinations
128-bit	3.4×10^{38}
192-bit	6.2×10^{57}
256-bit	1.1×10^{77}

Table X: AES Key Size to Possible Combinations (Arora, 2012, para. 5)

Key Size	Time to Enumerate all Keys
128-bit	1.02×10^{18} years
192-bit	1.872×10^{37} years
256-bit	3.31×10^{56} years

Table X: 10.51 Petaflop Supercomputer Key Enumeration for AES (Arora, 2012, para. 14)

To enumerate all keys possible AES 128-bit keys using a 2012 level supercomputer, it would take a billion-billion years (Arora, 2012, para. 14).

What are the cons of secret-key cryptography?

There must be an alternative secure channel to transmit keys. “All secret key algorithms or systems require that the party generating the key share or transfer it to the other party in a secure manner” (Shelton, 2015).

Strictly secret-key encryption implementation for large scale networks is not feasible. Having a network of computers all communicating with each other using secret-key cryptography requires $n(n-1)/2$ keys (Odlyzko, 1994, p. 19). 20 million users all using symmetric cryptography with one-another would require 200 trillion total keys (Odlyzko, 1994, p. 19). This is not practical and creates a very large storage overhead.

Ideas: Weaknesses could go here.

How do we solve the flaws in secret-key cryptography?

Public-key cryptography is the answer to the flaws of secret-key cryptography. We use public-key cryptography for key exchange, user/entity authentication, sender non-repudiation, and message authentication. In conjunction, we use public and secret-key cryptography together to begin fast, secure communication.

Ideas: Continue with this train-of-thought.

Public-Key Cryptography

Introduction

Public-key cryptography is a form of cryptograph that uses a pair of keys to encrypt and decrypt. This cryptosystem works by creating a public/private key-pair for every party. Each party will make their public-key openly accessible, and will store their private key for their eyes only. To send a message using public-key cryptography, a sender will encrypt their message using their recipient's public-key and then transmit the ciphertext to them. The recipient then decrypts the ciphertext with their private key.

Ideas: Redo this section – sloppy.

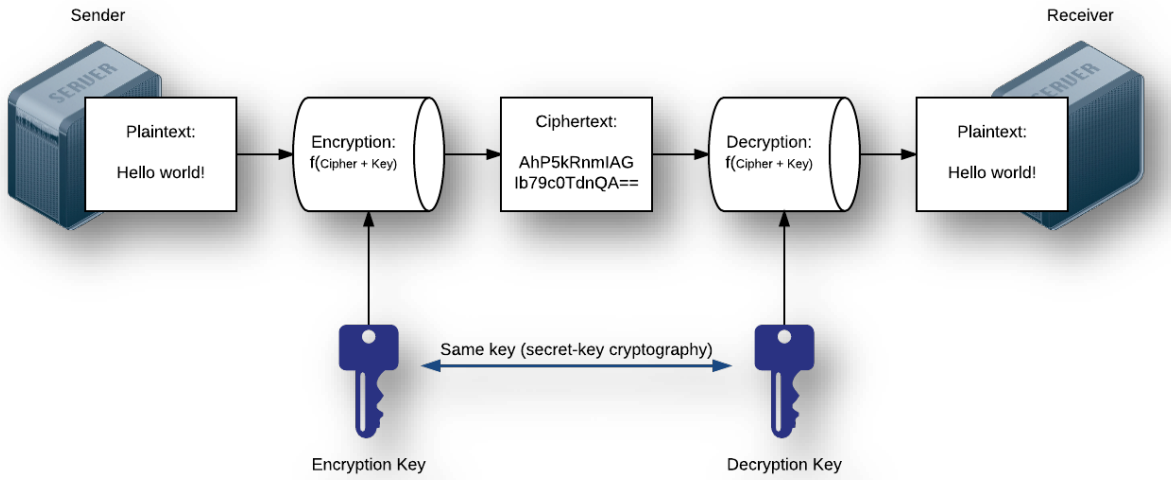


Fig. X. *Illustration of a Cryptosystem Implementing Public-Key Cryptography*

History

Ideas: there has been a need for this kind of cryptosystem for years. In the 1960s, Government Communications Headquarters (GCHQ) cryptographer James H. Ellis wrote a classified journal on the need for non-secret encryption (Barr, 2002, p. 243). However, in the 1970s, Stanford Researchers Whit Diffie, Ralph Merkle, and Martin Hellman invented the first public-key cryptosystem entitled Diffie-Hellman key exchange (Odlyzko, 1994, p. 19). It was not cryptographically sound. 1978, Ronald Rivest, Adi Shamir, and Leonard Adelman published their RSA public-key algorithm that is still in use today (Barr, 2002, p. 286).

What uses public-key cryptography?

Encrypted e-mail, Internet browsing using HTTP/Secure Sockets Layer (HTTPS), e-commerce, mobile banking, authentication of smart devices, citizen passports, and mass transit ticketing systems are a few real-world examples that use public-key cryptography (Moulds).

Ideas: continue to talk more about how a casual Internet user uses public-key daily.

What are the facets of public-key cryptography?

- *Key-Exchange*
  Public-key cryptography has enabled the ability for mass key exchange throughout the Internet without the need to store the inexplicably large number of keys it would take for secret-key encryption to achieve this purpose.

- *Authentication via Digital Signatures*
  Authentication is defined as obtaining the identification of the sender (Shelton, 2015). Digital Signatures reverse the typical sending process: sign a message with your private key and let others decrypt with your public key. This means it's guaranteed to have come from you and creates non-repudiation.

- *Sender Non-Repudiation*
  Non-repudiation is defined as the inability of a sender to refute that they signed something encrypted with their private key (Shelton, 2015).

- *Message Authentication*
  Hashing the message and attaching the hash to the message to provide integrity.

Ideas: Work out more specifics in this section and expound on these concepts.

Public-Key Examples

The RSA Cryptosystem

The methodology for RSA requires the use of prime numbers and modulus, but is still secure today (Odlyzko, 1994, p. 19).

Ideas: continue into RSA key sizes, applications today.

Key Exchange using RSA

Ideas: Finishing developing example diagrams and problem.

Digital Signatures using RSA

Ideas: Finishing developing example diagrams and problem.

Message Authentication

Ideas: Finishing developing example diagrams and problem.

Conclusion

For Final Copy

Ideas: summarize secret and private-key's applications to one another in diagram

References

Arora, M., Sr. (2012, May 7). How secure is AES against brute force attacks? Retrieved March 26, 2017, from http://www.eetimes.com/document.asp?doc_id=1279619

Barr, T. H. (2002). *Invitation to Cryptology*. Upper Saddle River, NJ: Prentice Hall.

Gaithuru J. N., Bakhtiari M., Salleh M., & Muteb A. M. (2015). A comprehensive literature review of asymmetric key cryptography algorithms for establishment of the existing gap. *2015 9th Malaysian Software Engineering Conference (MySEC)*, 236-244. doi: 10.1109/MySEC.2015.7475227

Gueron, S. (2012, August 2). Intel Advanced Encryption Standard (Intel AES) Instructions Set. Retrieved March 27, 2017, from https://software.intel.com/en-us/articles/intel-advanced-encryption-standard-aes-instructions-set

Hammond, J. (2015, April 24). Encryption 101: The Vigenère cipher. Retrieved March 21, 2017, from https://www.egress.com/en-US/blog/encryption-101-the-vigenere-cipher

Hasib, A. A., & Haque, A. A. M. M. (2008). A Comparative Study of the Performance and Security Issues of AES and RSA Cryptography. *2008 Third International Conference on Convergence and Hybrid Information Technology,2*, 505-510. doi:10.1109/iccit.2008.179

Krebs, B. (2015, August 18). How Not to Start an Encryption Company. Retrieved March 16, 2017, from https://krebsonsecurity.com/2015/08/how-not-to-start-an-encryption-company/

Moulds, R. (n.d.). What is a PKI and why is it important? Retrieved February 26, 2017, from https://www.thales-esecurity.com/blogs/2013/march/what-is-a-pki

Odlyzko, A. M. (1994). Public Key Cryptography. *AT&T Technical Journal, 73*(5), 17-23. doi:10.1002/j.1538-7305.1994.tb00606.x

Origin of Cryptography. (n.d.). Retrieved March 22, 2017, from https://www.tutorialspoint.com/cryptography/cryptography_quick_guide.htm

Schneier, B. (2012, March 22). Can the NSA Break AES? Retrieved March 26, 2017, from https://www.schneier.com/blog/archives/2012/03/can_the_nsa_bre.html

Shelton, B. K. (2015, November 11). Introduction to Cryptography. Retrieved February 26, 2017, from http://www.infosectoday.com/Articles/Intro_to_Cryptography/Introduction_Encryption_Algorithms.htm