Essay: Asymmetric Cryptography

November 7, 2018 by Essay Sauce

Preview of page one of this free downloadable essay:

Essay details:

- **Subject area(s):** Information technology essays
- **Number of words:** 2759
- **Price:** Free download
- **File format:** PDF

Overall rating: **0** out of **5** based on 0 reviews.

500 word text preview of this essay:

The full version of this essay has 2759 words and is available to download in PDF format above.

Research Paper

Residency Weekend Group Project

Asymmetric Cryptography Explained All at Once

Submitted to Dr. Donald Grimes by Residency Group 4

In partial fulfillment of course, requirement of EMSISS

ISOL535: Cryptography

University of the Cumberlands

Spring 2018

Abstract

In today's technology, securing a system is an essential issue. Numerous procedures are given to secure system. Cryptographic is a strategy of changing a message into such frame which is ambiguous, and afterward retransforming that message back to its unique shape. If you want to keep your information safe and secret, you have the possible strategies are: hide the existence of the information or make the information unintelligible. Cryptography is the art and science of keeping information secure from unintended audiences, of encrypting it. Cryptography is a method used to store and transmit data in a secret form so that only those for whom it is intended can read and process it.

Keywords: RSA (Rivest Shamir Aldeman), El-gamal, Asymmetric cryptography, Public Key.

INTRODUCTION

With the globalization in the e-commerce, where everything is digital and is done online, may it be online shopping, money transfer, e-banking, e-voting, e- registration, sending email, security is the main priority. Reliance on electronic communications makes information vulnerable to unauthorized users. Hence the users need confidentiality, message integrity, sender non-repudiation and sender and authentication

Cryptography Goals

Listed below are the five main reasons what Encryption is implemented for:

a. Authentication: This can be achieved in two ways: Peer entity Authentication and Data Origin Authentication

b. Privacy/Confidentiality: This is to protect data from unauthorized access, may it be whole messages, part of data and even existence of a message. With this, data transmission can be combatted via passive attacks.

c. Integrity: This is to ensure that the receiver receives the data just the way it was intended without any alteration. Basically, this is achieved by check sum of IPv4 packets.

d. Non-repudiation: When the message is transferred, the receiver can prove that it was sent by a particular sender. This confirms that neither sender or receiver denies for sending/receiving a message

e. Service Reliability and Availability: The online systems can easily be attacked by hackers, intruders and that can affect the services to the system users.

Asymmetric Cryptography

Asymmetric cryptography makes use of public & the private key for encrypting and decrypting the data. It is also known as public key cryptography. Keys can be defined as large numbers that are paired together, but they are not identical. The public key is the one that can be shared with anyone. Private Key is the one that is used as a secret. (Ronald, 1990) One of the keys is used for encrypting the data and other is used for the purpose of decryption. There are several protocols that are used for encryption & the digital signature function. It can be used in the software program like the web browser that can be used for establishing a secure connection over the insecure network or it can also be used for validating the digital signature. (Norman, 2008) As asymmetric encryption provides the authenticity, integrity, non-repudiation, and

confidentiality, then the system and the users should be certain the public key is authentic, and it has not tampered, and it belongs to the person claimed.

This concept makes use of the key pairs. Data that is encrypted by the public key can be decrypted by the private key so for the sender to send the encrypted message to the recipient, then senders need the public key of the recipient. (Ronald, 1990)

Bob & Alice needs to exchange the message using the insecure channel and there is need ensure that information that is sent can't be read by a 3rd party like Eve. Bob & Alice encrypts a message using asymmetric cryptography and for the same purpose, Bob needs the public key of the Alice. The public key can be viewed by anyone like Eve. The key becomes visible to the public through the public server or an email. In the same way as Bob, Using the public key of Alice, he can encrypt the message and can send to anyone. The message sent by Bob can be decrypted by a private key of the Alice. (Norman, 2008)

EXAMPLE OF ASYMMETRIC CRYPTOGRAPHY: CLEF

When a user signs up for the clef, then it generates the private & public key and sends the public key to the server. When a user logged in, then a message is sent with the private key to the server. The message that is sent by private key can be verified using public key and only private key can generate the message. Hence, if the attacker has the public key even then he can't log in its system as they need the private key that gets generated on the phone and stored as encrypted on the phone and does not get transmitted. (Ronald, 1990)

STRENGTHS OF ASYMMETRIC CRYPTOGRAPHY

a. Message authentication: It allows the use of the digital signature, so the recipient of the message can be verifying that message truly comes from the specific sender.

b. Convenience: It solves the problem about the distribution keys for the encryption where public keys are published, and private ones are kept as secret.

c. Non-repudiation: The messages are digitally signed just like the physical ones, so it acknowledges the message and sender can't deny it. (Ayushi, 2010).

d. Detection of tampering: In asymmetric cryptography, digital signatures are used so the recipient of the message can detect if the message is altered or not.

WEAKNESSES OF ASYMMETRIC CRYPTOGRAPHY

1. Slow process: Asymmetric cryptography is a slow process as compared to the symmetric cryptography, so it is not a suitable method to decrypt the bulk messages.

2. The authenticity of public keys: Public keys are not authenticated as no one knows that key belongs to the specific individual, so the user needs to very that public key belongs to them.

3. Private Key loss: In case of loss of the private key then received messages can't be decrypted. (Norman, 2008)

4. Security compromise: If the private key gets identified by the attacker then he can read all the messages.

ALGORITHMS THAT IMPLEMENT ASYMMETRIC CRYPTOGRAPHY

RSA ALGORITHM

It is the most proven and employed one. It was invented by 3 scholars, Ron Rivest, Len Adleman and Aid Shamir.

RSA Key pair: When a user needs to participate in communication by using encryption then there is a need to generate a pair of keys and they are private and public keys. (Ayushi, 2010) There is a process that is followed in keys generations. Firstly, the RSA modulus is generated and then the derived number is found out then public key is formed and the private key is generated.

Encryption / Decryption: Once the pair of key gets generated then the process of encryption or decryption are carried out. RSA operated on numbers modulo n. The plain text is represented as series of numbers that are less than n. (Ronald, 1990)

RSA encryption: If the sender wants to send a text message to someone with a public key (n,e) then sender represent plain text as a series of numbers that are less than n. P
laintext P is encrypted using C = P^e mod n.

Cipher text C is equivalent to plaintext P that is multiplied itself e times and it is reduced modulo n.

RSA decryption: It is a straightforward method. If the receiver has a public key pair (n,e) and cipher text C. C is raised to the power of private key d and result modulo n is plaintext P. (Ayushi, 2010)

RSA Analysis: RSA security depends on the strength of Encryption function and key generation. It is most popular one. The encryption function is a one-way function to convert plain into cipher-text and can be reversed using private key d. Difficult to determine private key from RSA public key is factoring modulus n.

DIFFIE HELLMAN KEY EXCHANGE ALGORITHM

It is called as an exponential key exchange. It is a method to digital encryption that makes use of numbers that are raised to some power to get decryption key that is based on components that do not get transmitted directly. (Ronald, 1990) Two users Alice and Bob are communicating with each other over the private channel and they mutually agree on some positive whole numbers, let's say, p & q and p is prime number & q is a generator of it. q is when raised to positive whole number power that is less than p never produces the same output for any two whole numbers. (Ayushi, 2010)

They do not divulge the personal key to anyone and they memorize time. Both of them compute the prima key on the basis of the formula.

a* = qa mod p

and

b* = qb mod p

They share their public key over communication medium like the internet. From these key, number x is generated by either of them on the basis of personal keys. (Ronald, 1990)

Alice computes

x = (b*)a mod p

and Bob computes:

x = (a*)b mod p

Value of x will be same and both of them can communicate privately over public medium with encryption method using decryption key x.

STRENGTHS OF DIFFIE HELLMAN KEY EXCHANGE:

1. It is an exponential key exchange and digital encryption method.

WEAKNESS OF DIFFIE HELLMAN KEY EXCHANGE:

1. They need to agree on the value of p & q as they chose personal keys a & b.

DIGITAL SIGNATURE ALGORITHM

It is used by the recipient of the message to ensure that message does not get altered during transmission and the identity of the originator is not certain. It is the electronic version of a written signature that can use to prove to the recipient that message was signed by the originator. It may be generated for stored programs and data so data and program integrity can be verified later on. (Ayushi, 2010)

Process:

1. Message digest gets encrypted by private key of the Bob and it is a digital signature.

2. Digital signatures get attached to message and then sent to Alice.

3. Alice verified it by decryption signature using public key and its result in message digest. (Ronald, 1990)

4. Alice hashes message and results in message digest. It both the message digest are same then Alice makes sure that Bob signed the message and it is not altered.

5. The encryption algorithm that is used ensures the confidentiality and hashing algorithm ensures the integrity of data. Digital Signing of documents ensures that message is authenticated, and it ensures the non-repudiation.

It enforces features of confidentiality, authentication, and non-repudiation. They ensure the authenticity of the business transactions. It makes use of the public key encryption. It is a string of bits. Let's consider an example where Bob wants to send digitally signed a message to Alice. Digital signature makes use of public key encryption where Bob and Alice have a public-private key pair. Some steps are followed for creating a digital signature and use it to send and receive messages between them. (Ayushi, 2010)

STRENGTHS OF DIGITAL SIGNATURE ALGORITHM:

1. It has the feature of Message authentication, Non-repudiation, Data integrity. It is an electronic version of the written signature that can be used to prove the recipient that message was signed by the originator.

WEAKNESS OF DIGITAL SIGNATURE ALGORITHM:

1. It makes use of the public key encryption.

Modern Applications that utilize Asymmetric Cryptography

X.509 is a standard describing a system that can be used for encryption, digital signatures, etc. Basically, a certificate is like a digital ID card – it verifies that you are who you say you are, at least according to the group or individual that issued the certificate. These certificates are used for secure web browsing, and can be used for signing and/or encrypting email using a variety of email programs (specifically Mail.app in Panther, in my case). X.509 email is used in the S/MIME standard. This is similar to, but incompatible with, PGP/MIME.

In cryptography, X.509 is an important standard for a public key infrastructure (PKI) to manage digital certificates, public-key encryption and a key part of the Transport Layer Security protocol used to secure web and email communication. An ITU-T standard, X.509 specifies formats for public key certificates, certificate revocation lists, attribute certificates, and a certification path validation algorithm. An X.509 certificate is a digital certificate that uses the widely accepted international X.509 public key infrastructure (PKI) standard to verify that a public key belongs to the user, computer or service identity contained within the certificate.

Structure of X.509 Certificate

Another Application of Asymmetric Encryption (iOS Data Security)

Asymmetric key encryption describes a class of algorithms using a a public and private key pair, to encrypt and decrypt. The public key can be used to decrypt data that was encrypted by the private key, and vice-versa.

This solves the key transmission problem with symmetric encryption because the private is never transmitted, only the public key. Once someone has the public key they can be sent data that has been encrypted using the private key.

The Diffie-Hellman key exchange method is a good example of using symmetric and asymmetric keys together. When two parties open a secure communication channel they start off using Public key encryption only long enough to agree upon a symmetric session (ephemeral) key, which will be used to encrypt further communication. Since the communication is encrypted with an ephemeral key, disclosure of the private asymmetric key will not allow decrypting of old messages.

Why industry choose Asymmetric Encryption over Symmetric Encryption despite being slower.

The issue with secret keys is trading them over the Internet or an extensive system while keeping them from falling into the wrong hands. Any individual who knows the secret key can decode the message. One answer is awry encryption, in which there are two related keys- – a key match. An open key is made uninhibitedly accessible to any individual who should need to send you a message. A moment, private key is kept secret, with the goal that lone you know it.

Any message (content, double records, or reports) that are encoded by utilizing public key must be decoded by applying a similar calculation, however by utilizing the coordinating private key. Any message that is encoded by utilizing the private key must be unscrambled by utilizing the coordinating public key.

This implies you don’t need to stress over ignoring public keys the Internet (the keys should be open). An issue with deviated e
ncryption, notwithstanding, is that it is slower than symmetric encryption. It requires significantly all the more preparing energy to both encode and unscramble the substance of the message.

CONCLUSION

Asymmetric cryptography can be used in the software program like the web browser that can be used for establishing a secure connection over the insecure network or it can also be used for validating the digital

signature. (Ronald, 1990) Data that is encrypted by the public key can be decrypted by the private key so for the sender to send the encrypted message to the recipient, then senders need the public key of the recipient. Digital signature makes use of the public key encryption. It is the practical application of Symmetric cryptography. Digital signature makes use of public key encryption. SSL is a practical application of Asymmetric cryptography. It uses public and private key pair and a symmetric session key that is one-time use key that is used for the purpose of encryption and the decryption. (Norman, 2008)

References

Rivest, Ronald L. (1990). "Cryptography". In J. Van Leeuwen. Handbook of Theoretical Computer Science

Doctorow, Cory (2 May 2007). "Digg users revolt over AACS key". Boing Boing. Retrieved 26 March 2015

Biggs, Norman (2008). Codes: An introduction to Information Communication and Cryptography. Springer. p. 171.

Delfs, Hans & Knebl, Helmut (2007). "Symmetric-key encryption". Introduction to cryptography: principles and applications. Springer. ISBN 9783540492436.

Mullen, Gary & Mummert, Carl (2007). Finite fields and applications. American Mathematical Society. p. 112. ISBN 9780821844182.

Ayushi (2010). "A Symmetric Key Cryptographic Algorithm" (PDF). International Journal of Computer Applications. 1-No 15.

Pelzl & Paar (2010). Understanding Cryptography. Berlin: Springer-Verlag. p. 30.

https://www.surf.nl/binaries/content/assets/surf/en/knowledgebase/2010/rapport_201009_SNcryptoWEB.pdf

https://support.microsoft.com/en-us/help/246071/description-of-symmetric-and-asymmetric-encryption

https://developer.apple.com/documentation/security/certificate_key_and_trust_services/keys/using_keys_for_encryption

https://sachi73blog.wordpress.com/2013/11/21/x509-certificate-asymmetric-encryption-and-digital-signatures/

https://www.slideshare.net/lalitasuwanvichien/9164-it346-wk32-27220055?next_slideshow=1

https://thesai.org/Downloads/Volume8No6/Paper_59-Cryptography_A_Comparative_Analysis_for_Modern_Techniques.pdf

http://accentsjournals.org/PaperDirectory/Journal/TIS/2016/1/5.pdf

https://pdfs.semanticscholar.org/5711/556af6e5edcc4432dc7a48fc5a3688bc3612.pdf

About Essay Sauce

EssaySauce.com is a completely free resource to help students research their academic work and learn from great essays!

View all posts by Essay Sauce

...(download the rest of the essay above)

Search for student essays:

Search ...

About EssaySauce, the student essay site:

EssaySauce.com is a free resource for students, providing thousands of example essays to help them complete their college and university coursework. Students can use our free essays as examples to write their own.

Latest student essays:

Harnessing energy through knowledge – business development strategy of e-commerce companies

Minimizing of power losses for distribution system

Translating the Biggles Stories for Czech Readers: A Case of Moderate Transposition

Questioning is a Useful Form of AfL

Enhancing literacy

Cadburys
Advancements in Procurement Practices and Supply-Chain Management...
LITERARY REVIEW – fashion industry
Chlorpyrifos
Get out of my space – business idea

Student essay categories:

Accounting essays
Architecture essays
Business essays
Economics essays
Education essays
Engineering essays
English language essays
English literature essays
Environmental studies essays
Finance essays
Health essays
History essays
Information technology essays
International Relations
Law essays
Literature essays
Management essays
Marketing essays
Miscellaneous essays
Music Essays
Photography and arts essays
Politics essays
Project management
Psychology essays
Religious studies and Theology essays
Science essays
Sociology essays
Zoology essays

Average review:

Overall rating: **0** out of **5** based on 0 reviews.

Q: Is EssaySauce.com free?

Yes! EssaySauce.com is a completely free resource for students. You can view our **terms of use** here.

Why use Essay Sauce?

The brightest students know that the best way to learn is by example! EssaySauce.com has thousands of great essay examples for students to use as inspiration when writing their own essays.

Is Essay Sauce completely free?

Yes! EssaySauce.com is a completely free resource for students. You can view our terms of use here.

Info:

About
Content policy
Essay removal request
Privacy
Terms of use