Introduction

The principal objectives of this had been to more concentrate on the confidentiality phase & it helps to discover the approach (ciphers) to make certain privacy via the use of DNA. DNA Cryptography is one of the most essential & promising disciplines in information security.

The RSA algorithm is regarded as a robust asymmetric encryption algorithm. Asymmetric cryptography, also known as public-key cryptography, is a process that uses a pair of related keys -- one public key and one private key -- to encrypt and decrypt a message and protect it from unauthorized access or use. RSA has the more security; thus, the algorithm is proved to be cryptographically secure and it is suitable for applications where more than one layer of security is required.

OTP is used for key generation purpose which offers the total privacy for the ciphertext then it helps the user to encryption scheme which has proved to be unbreakable.

The transferring information from one node to another node by using the MAC address it is very safe and secure as every device has its unique address in its DNA Cryptography Encryption.

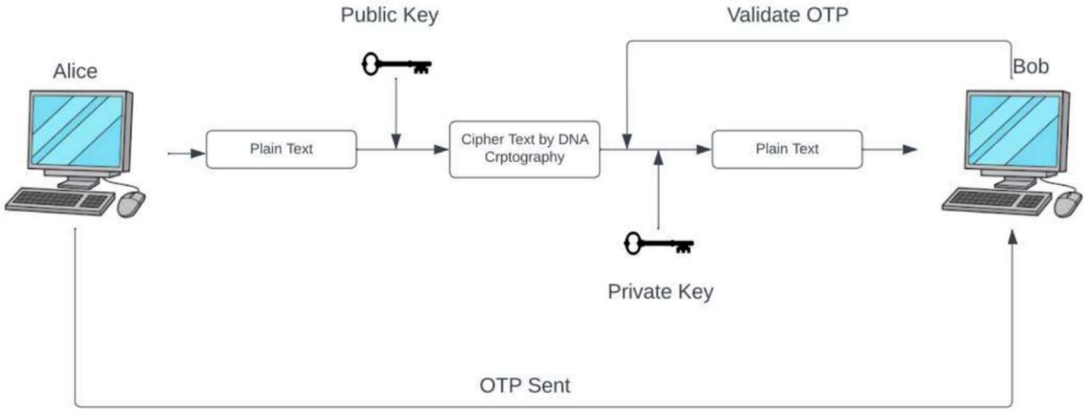
Literature Survey

S. No.	Title of Paper	Author and Journal Name	Objectives of the Paper	Methodologies Used	Results Obtained	Limitations
1.	"A Dynamic DNA Cryptography Using RSA Algorithm and OTP"	Poojashree Kamble,Firoz Nagarchi,Akshata Akkole,Vanishree Khanapur,Bahubali Akiwate, International Journal of Scientific Research in Computer Science and Engineering	In this approach, the encryption and the decryption take place through RSA Algorithm and the OTP. The use of a combination of DNA with RSA ensures twofold protections in a cloud environment where there are greater probabilities of breaches.	RSA Algorithm DNA Encoding Algorithm One Time Pad Key Generation	A robust Cryptography Technique using DNA Encryption and OTP System	In future the network can be connected with a greater number of nodes with both IP Address and MAC address with improvement in performance. Proposed File size only up to 100MB. Only 4-digit OTP, can be guessed easily by a fast-computing machine.
2.	"A Research Paper on Cryptography"	Gurdeep Singh, Prateek Kumar, International Journal for Technological Research in Engineering	Abstract Data Types, Data Encryption, Data Compression, Asymmetric Key Cryptography	Symmetric and Asymmetric Encryption and Decryption	Cryptography is used to ensure that the contents of a message are confidentiality transmitted and would not be altered.	If the attacker will get the key and sender and receiver is not aware about it it may harm the CIA triad. So, proper method should be used to Encrypt and Decrypt the data.
3.	"Research Paper on Cyber Security"	Mrs. Ashwini Sheth, Mr. Sachin Bhosale & Mr. Farish Kurupkar, Contemporary Research in India	In the current world of technology, it is crucial to know what Cyber Security is and how to use it effectively. How to Secure Systems, important files, data and other important virtual things.	1)Symmetric and Asymmetric Encryption 2) Types of Phishing: -Ransomware, Malware. 3)Goals of Cyber Security: Confidentiality, Integrity, Availability. 4)Attacks on IOT	Awareness on Online Attacks, Types of Viruses, Goals of Cyber Security, Advantages and Disadvantages of Cyber Security	Increasing Threats targeting user devices, devices used by employees who are working from home aren't protected well enough from attacks and preventing hackers.
4.	"A Study on Cryptographic Techniques"	Anjali Krishna A, Dr. L C Manikandan, International Journal of Scientific Research in Computer Science, Engineering and Information Technology	Data security using Symmetric and Asymmetric Key Encryption.	Symmetric and Asymmetric Key Encryption	There are different techniques and algorithms researched, and various types of work have been performed. In this paper briefly discussed cryptography and its form of symmetric key cryptography and algorithms for asymmetric key cryptography.	Key leakage, software bugs, holes in operating systems, side-channel attacks, phishing attacks, and social engineering. So, it is important to understand and acknowledge that cryptography ≠ security. Nevertheless, when cryptography fails, the consequences can be very severe.

This paper discusses about the Limitations of Paper in the table. The OTP generated is of only 4 digits which can be easily guessed by a fast-computing machine in a matter of mere seconds (even milli seconds).

The data to be encrypted (and also condensed) can only be of 100MB which is Trivial in most cases. We shall attempt to successfully rectify these limitations and provide for a stronger encryption built on the base of this journal.

Architecture Diagram



Working of the Algorithm

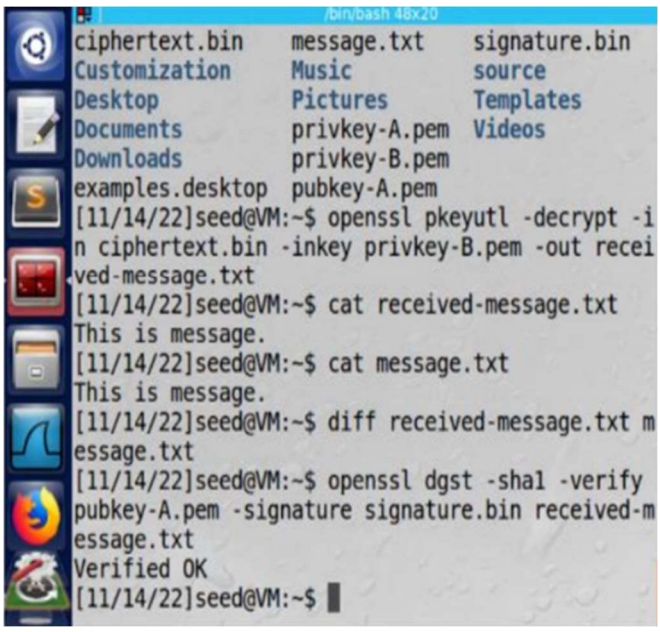
Table 1: DNA sequences in binary form

Binary Digits	DNA Base
00	A
01	G
10	C
11	T

Table 2: DNA encoding sequences

space → CCAG	! → CACT	" → TCGA	# → GTAC
(→ GCTG	) → CGTG	* → ATGG	+ → TGTA
, → AAAT	- → GGCC	. → TGGG	/ → TCCT
0 → CGCT	1 → TCAC	2 → GAGG	3 → CTAC
4 → CCTC	5 → CCTT	6 → AAAG	7 → GGGT
8 → TTGT	9 → TAAT	: → AGGG	; → GTTT
< → GTGT	= → CAAG	> → AACA	? → CTTG
@ → CAAA	A → TGTT	B → CAAC	C → TTAA
D → GAAA	E → CCTG	F → TGAG	G → ACCC
H → CCCC	I → GGAT	J → TGGT	K → CAGA
L → CTTC	M → ATAC	N → CCAA	O → GGCA
P → TGAA	Q → CTGG	R → GGGC	S → GCTA
T → CCCG	U → GGAA	V → AGAC	W → ACTG
X → GCAT	Y → ACCT	Z → TCTT	[→ CGTT
\ → TGGC	] → CTAT	^ → AGGA	_ → AGAA
` → ACGG	a → CTCT	b → GGTG	c → GGAG
d → TAAA	e → GCCA	f → GACC	g → GTGA
h → TGCT	i → ATAT	j → GAGA	k → CAGT
l → AATT	m → TTGG	n → GTAG	o → TCTC
p → TTTG	q → TTCC	r → GTCT	s → AGTT
t → ACAC	u → GCAA	v → TTCT	w → TCAA
x → GGTC	y → TCTG	z → AAGA	{ → GCTT
| → GTGC	} → CCCA	~ → ATGT	

RSA Key Generation, Signatures and Encryption using OpenSSL



Abstract

The most distinct feature of Public Key Infrastructure (PKI) is that it uses a pair of keys to achieve the underlying security service. The key pair comprises of private key and public key.

Since the public keys are in open domain, they are likely to be abused. It is, thus, necessary to establish and maintain some kind of trusted infrastructure to manage these keys.

Key Management

It goes without saying that the security of any cryptosystem depends upon how securely its keys are managed. Without secure procedures for the handling of cryptographic keys, the benefits of the use of strong cryptographic schemes are potentially lost.

It is observed that cryptographic schemes are rarely compromised through weaknesses in their design. However, they are often compromised through poor key management.

There are some important aspects of key management which are as follows − Cryptographic keys are nothing but special pieces of data. Key management refers to the secure administration of cryptographic keys.

Introduction

PKI provides assurance of public key. It provides the identification of public keys and their distribution. An anatomy of PKI comprises of the following components.

- Public Key Certificate, commonly referred to as 'digital certificate'.
- Private Key tokens.
- Certification Authority.
- Registration Authority.
- Certificate Management System.

There are two specific requirements of key management for public key cryptography.

- Secrecy of private keys: Throughout the key lifecycle, secret keys must remain secret from all parties except those who are owner and are authorized to use them.
- Assurance of public keys: In public key cryptography, the public keys are in open domain and seen as public pieces of data. By default, there are no assurances of whether a public key is correct, with whom it can be associated, or what it can be used for. Thus, key management of public keys needs to focus much more explicitly on assurance of purpose of public keys.

The most crucial requirement of 'assurance of public key' can be achieved through the public-key infrastructure (PKI), a key management system for supporting public-key cryptography.

For analogy, a certificate can be considered as the ID card issued to the person. People use ID cards such as a driver's license, passport to prove their identity. A digital certificate does the same basic thing in the electronic world, but with one difference.

Digital Certificates are not only issued to people but they can be issued to computers, software packages or anything else that need to prove the identity in the electronic world.

Digital certificates are based on the ITU standard X.509 which defines a standard certificate format for public key certificates and certification validation. Hence digital certificates are sometimes also referred to as X.509 certificates.

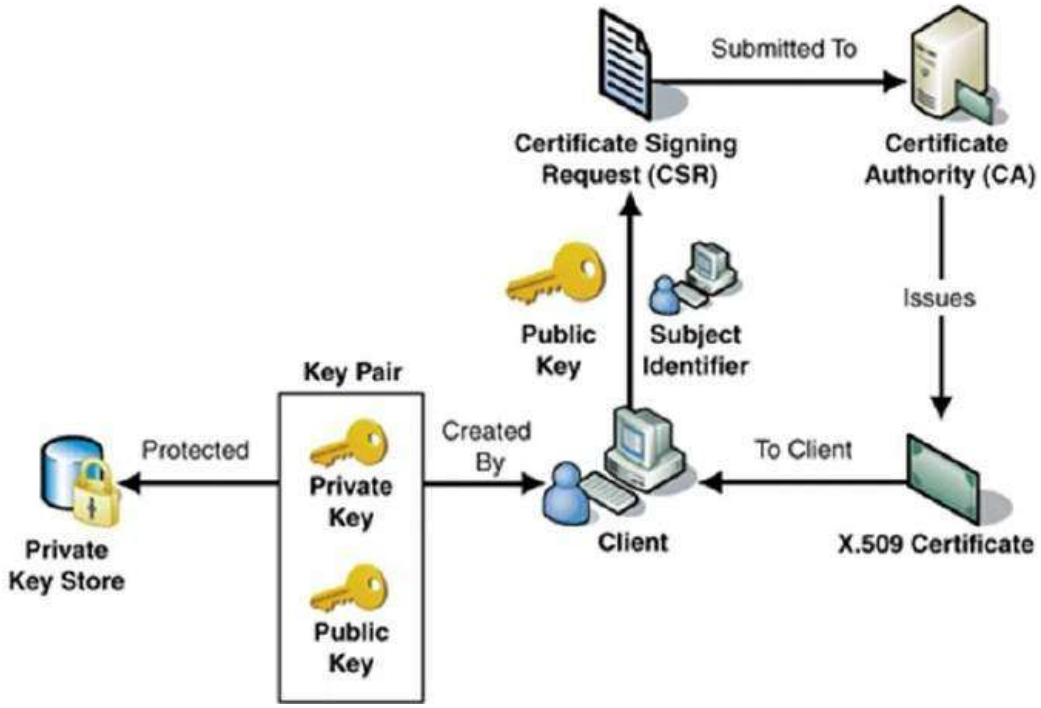
Public key pertaining to the user client is stored in digital certificates by The Certification Authority (CA) along with other relevant information such as client information, expiration date, usage, issuer etc.

- CA digitally signs this entire information and includes digital signature in the certificate.

- Anyone who needs the assurance about the public key and associated information of client, he carries out the signature validation process using CA's public key. Successful validation assures that the public key given in the certificate belongs to the person whose details are given in the certificate.

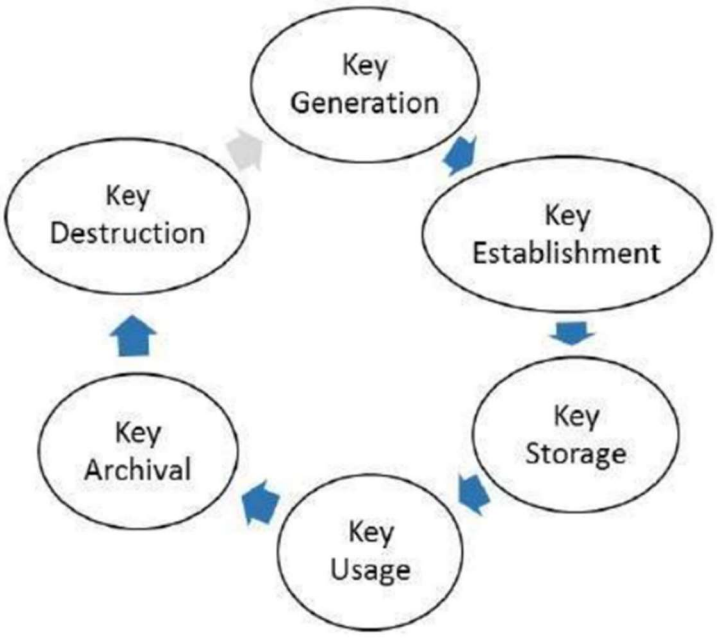
Proposed Model

Architecture: - The process of obtaining Digital Certificate by a person/entity is depicted in the following illustration.



As shown in the illustration, the CA accepts the application from a client to certify his public key. The CA, after duly verifying identity of client, issues a digital certificate to that client.

Explanation: - Key management deals with entire key lifecycle as depicted in the following illustration –



Certifying Authority (CA)

As discussed above, the CA issues certificate to a client and assist other users to verify the certificate. The CA takes responsibility for identifying correctly the identity of the client asking for a certificate to be issued, and ensures that the information contained within the certificate is correct and digitally signs it.

Key Functions of CA

The key functions of a CA are as follows –

- Generating key pairs − The CA may generate a key pair independently or jointly with the client.
- Issuing digital certificates − The CA could be thought of as the PKI equivalent of a passport agency − the CA issues a certificate after client provides the credentials to confirm his identity. The CA then signs the certificate to prevent modification of the details contained in the certificate.
- Publishing Certificates − The CA need to publish certificates so that users can find them. There are two ways of achieving this. One is to publish certificates in the equivalent of an electronic telephone directory. The other is to send your certificate out to those people you think might need it by one means or another.
- Verifying Certificates − The CA makes its public key available in environment to assist verification of his signature on clients' digital certificate.
- Revocation of Certificates − At times, CA revokes the certificate issued due to some reason such as compromise of private key by user or loss of trust in the client. After revocation, CA maintains the list of all revoked certificate that is available to the environment.

Classes of Certificates

There are four typical classes of certificate –

- Class 1 − These certificates can be easily acquired by supplying an email address.
- Class 2 − These certificates require additional personal information to be supplied.
- Class 3 − These certificates can only be purchased after checks have been made about the requestor's identity.

- Class 4 − They may be used by governments and financial organizations needing very high levels of trust.

Registration Authority (RA)

CA may use a third-party Registration Authority (RA) to perform the necessary checks on the person or company requesting the certificate to confirm their identity. The RA may appear to the client as a CA, but they do not actually sign the certificate that is issued.

Certificate Management System (CMS)

It is the management system through which certificates are published, temporarily or permanently suspended, renewed, or revoked. Certificate management systems do not normally delete certificates because it may be necessary to prove their status at a point in time, perhaps for legal reasons. A CA along with associated RA runs certificate management systems to be able to track their responsibilities and liabilities.

Private Key Tokens

While the public key of a client is stored on the certificate, the associated secret private key can be stored on the key owner's computer. This method is generally not adopted. If an attacker gains access to the computer, he can easily gain access to private key. For this reason, a private key is stored on secure removable storage token access to which is protected through a password.

Different vendors often use different and sometimes proprietary storage formats for storing keys. For example, Entrust uses the proprietary .epf format, while Verisign, GlobalSign, and Baltimore use the standard .p12 format.

Hierarchy of CA

With vast networks and requirements of global communications, it is practically not feasible to have only one trusted CA from whom all users obtain their certificates. Secondly, availability of only one CA may lead to difficulties if CA is compromised.

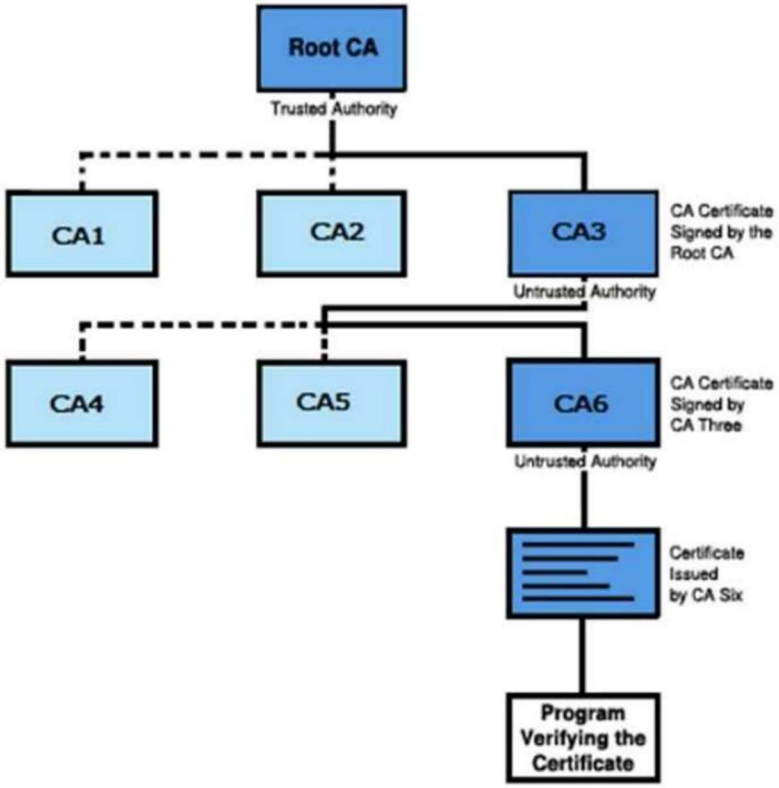
In such case, the hierarchical certification model is of interest since it allows public key certificates to be used in environments where two communicating parties do not have trust relationships with the same CA.

- The root CA is at the top of the CA hierarchy and the root CA's certificate is a self-signed certificate.

- The CAs, which are directly subordinate to the root CA (For example, CA1 and CA2) have CA certificate s that are signed by the root CA.
- The CAs under the subordinate CAs in the hierarchy (For example, CA5 and CA6) have their CA certificates signed by the higher-level subordinate CAs.

Certificate authority (CA) hierarchies are reflected in certificate chains. A certificate chain traces a path of certificates from a branch in the hierarchy to the root of the hierarchy.

The following illustration shows a CA hierarchy with a certificate chain leading from an entity certificate through two subordinate CA certificates (CA6 and CA3) to the CA certificate for the root CA.



Verifying a certificate chain is the process of ensuring that a specific certificate chain is valid, correctly signed, and trustworthy. The following procedure verifies a certificate chain, beginning with the certificate that is presented for authentication –

- A client whose authenticity is being verified supplies his certificate, generally along with the chain of certificates up to Root CA.
- Verifier takes the certificate and validates by using public key of issuer. The issuer's public key is found in the issuer's certificate which is in the chain next to client's certificate.

- Now if the higher CA who has signed the issuer’s certificate, is trusted by the verifier, verification is successful and stops here.
- Else, the issuer's certificate is verified in a similar manner as done for client in above steps. This process continues till either trusted CA is found in between or else it continues till Root CA.

Conclusion

In this tutorial we discussed the basics of the science of Public Key. It explains how programmers and network professionals can use cryptography to maintain the privacy of computer data. Starting with the origins of cryptography, it moves on to explain cryptosystems, various traditional and modern ciphers, public key encryption, data integration, message authentication, and digital signatures.

Reference

1. E. M. S. Hossain, K. M. R. Alam, M. R. Biswas and Y. Morimoto, "A DNA cryptographic technique based on dynamic DNA sequence table," 2016 19th International Conference on Computer and Information Technology (ICCIT), 2016, pp. 270-275, doi: 10.1109/ICCITECHN.2016.7860208.
2. M. R. Biswas, K. M. R. Alam, A. Akber and Y. Morimoto, "A DNA cryptographic technique based on dynamic DNA encoding and asymmetric cryptosystem," 2017 4th International Conference on Networking, Systems and Security (NSysS), 2017, pp. 1-8, doi: 10.1109/NSYSS2.2017.8267782.
3. Vinay S, Adarsh Pujar, Ankith, H.Akshay Kedlaya, Vasudev S Shahapur, 2019, Implementation of DNA Cryptography based on Dynamic DNA Sequence Table using Cloud Computing, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) RTESIT – 2019 (VOLUME 7 – ISSUE 08)
4. Bahubali Akiwate, Latha Parthiban, A Dynamic DNA for Key-based Cryptography, CTEMS, IEEE, 2018.