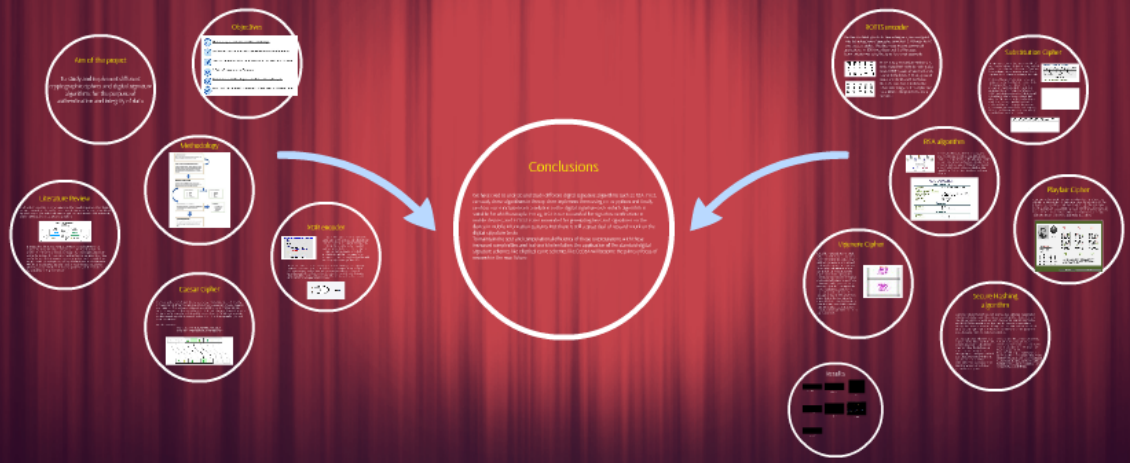
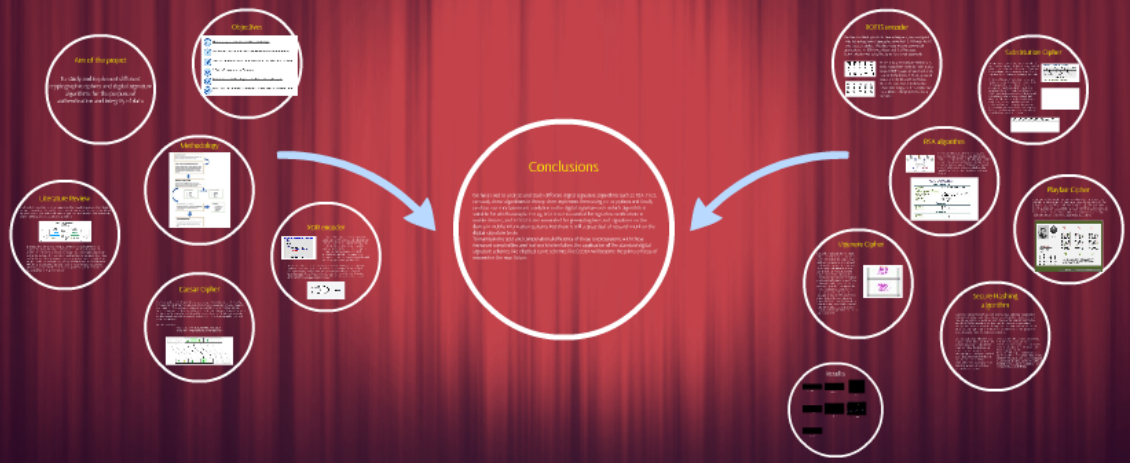
Digital Signatures: Applications and Implementations



Prezi

Digital Signatures: Applications and Implementations

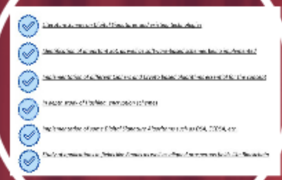


Prezi

Aim of the project

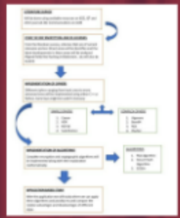
To study and implement different cryptographic ciphers and digital signature algorithms for the purpose of authentication and integrity of data

Objectives

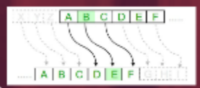


Literature Review

Methodology



Caesar Cipher



XOR encoder

C

We have tried to analyze and stu
we study these algorithms in the
we draw our conclusions on a so
suitable for which example. For
mobile devices, and ECDSA is re
device in mobile information sys
digital signature to do.
To maintain the cost and compu
increased complexities and real-
signature schemes like elliptical
research in the near future.

Prezi

Aim of the project

To study and implement different cryptographic ciphers and digital signature algorithms for the purpose of authentication and integrity of data

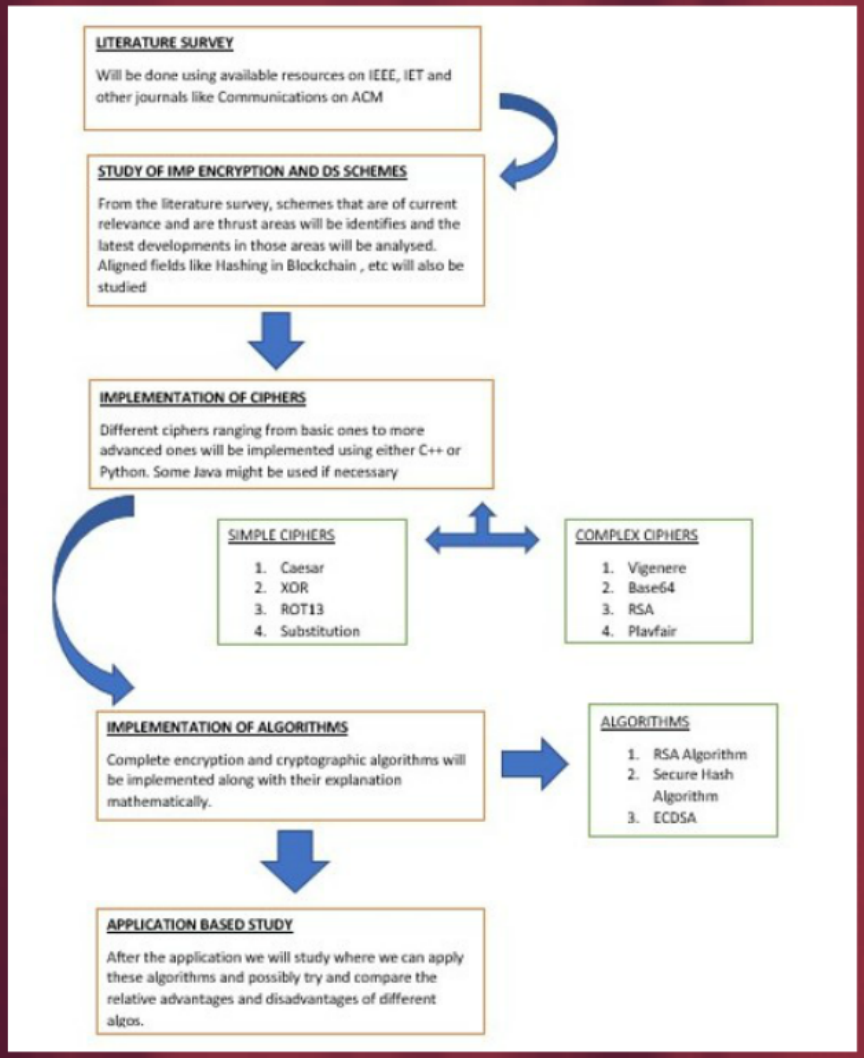
Prezi

Objectives

- *Literature Survey on Digital Signatures and existing technologies*
- *Identification of important SoC as well as software-based schemes being implemented*
- *Implementation of different Ciphers and Crypto based algorithms essential for the concept*
- *In depth study of Hashing, encryption schemes*
- *Implementation of some Digital Signature Algorithms such as DSA, ECDSA, etc.*
- *Study of applications in fields like Emails as well as aligned prosperous fields like Blockchain*

Prezi

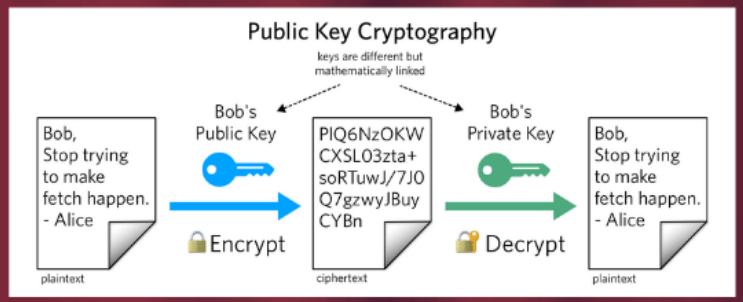
Methodology



Prezi

Literature Review

Ulrich Pordesch, a German researcher viewed it a risk to have other agencies verify and sign a document, “imbedding and using the schemes in application systems involves considerable risks in particular, if the signer or the verifier uses an application environment which is maintained, used, or controlled, by other persons or organizations.”



Cryptography is divided into two types, Symmetric key and Asymmetric key cryptography. In Symmetric key cryptography a single key is shared between sender and receiver. The sender uses the shared key and encryption algorithm to encrypt the message. The receiver uses the shared key and decryption algorithm to decrypt the message. In Asymmetric key cryptography each user is assigned a pair of keys, a public key and a private key. The public key is announced to all members while the private key is kept secret by the user. The sender uses the public key which was announced by the receiver to encrypt the message. The receiver uses his own private key to decrypt the message

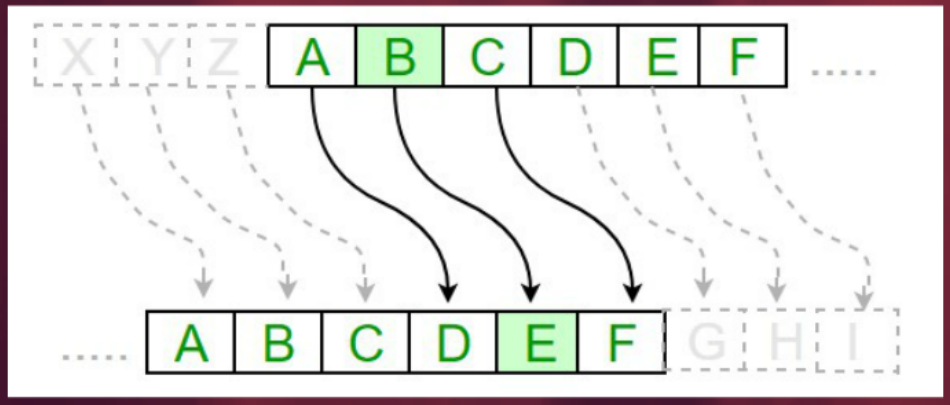
Prezi

Caesar Cipher

The Caesar cipher is named after Julius Caesar, who, according to Suetonius, used shift cipher with a constant left shift of 3 to encrypt important military messages during the war. Hence it is also known as shift cipher, Caesar's cipher or Caesar shift. It uses a substitution method to evolve the encrypted text. The Caesar cipher is one of the earliest known and simplest ciphers. It is a type of substitution cipher in which each letter in the plaintext is 'shifted' a certain number of places down the alphabet. For example, with a shift of 1, A would be replaced by B, B would become C, and so on.

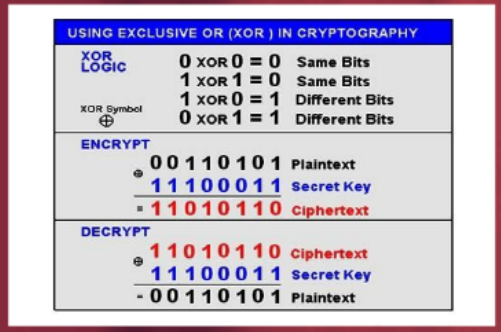
Consider an Example,

Plain text: ZYXWVUTSRQPONMLKJIHGFEDCBA
Cipher text: WVUTSRQPONMLKJIHGFEDCBAZYX



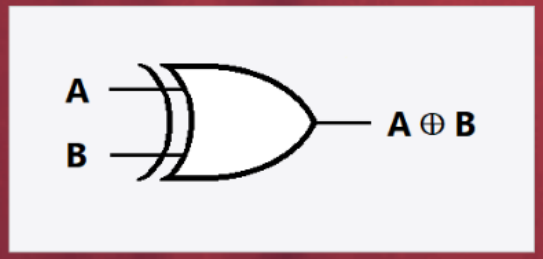
Prezi

XOR encoder



Exclusive-OR encryption, while not a public-key system such as RSA, is almost unbreakable through brute force methods. It is susceptible to patterns, but this weakness can be avoided through first compressing the file (so as to remove patterns). Exclusive-or encryption requires that both encryptor and decryptor have access to the encryption key, but the encryption algorithm, while extremely simple, is nearly unbreakable.

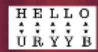
The actual way exclusive-OR encryption is used is to take the key and encrypt a file by repeatedly applying the key to successive segments of the file and storing the output. The output will be the equivalent of an entirely random program, as the key is generated randomly. Once a second person has access to the key, that person is able to decrypt the files, but without it, decryption is almost impossible. For every bit added to the length of the key, you double the number of tries it will take to break the encryption through brute force.



Prezi

ROT13 encoder

The treasure hunting website, Geocaching.com, uses encrypted hints to the locations of geocaches using ROT13. Although ROT13 is not a secure cipher, it has been used in some commercial applications. In 1999 it was discovered that Netscape Communicator was using the cipher to encrypt passwords



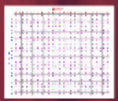
ROT13 is easy to translate without any tools. If you think might be looking at a piece of ROT13 code, all you need to do is to write the letters A-M on a piece of paper, and the letters N to Z below them. You can then substitute the letters accordingly, so if the cipher text has a letter A, the plain text is N and vice versa

Substitution Cipher

RSA algorithm

Playfair Cipher

Vigenere Cipher



Secure Hashing algorithm

Results

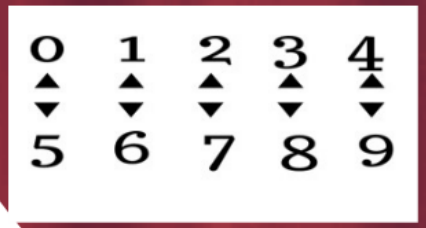
algorithms such as RSA. First,
ing c++ or python and finally,
as to which algorithm is
ignature verification on
eys and signatures on the
deal of research work on the

yptosystems with these
tion of the standard digital
ll become the primary focus of

Prezi

ROT13 encoder

The treasure hunting website, Geocaching.com, uses encrypted hints to the locations of geocaches using ROT13. Although ROT13 is not a secure cipher, it has been used in some commercial applications. In 1999 it was discovered that Netscape Communicator was using the cipher to encrypt passwords



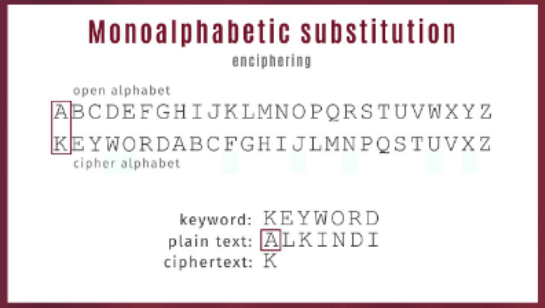
ROT13 is easy to translate without any tools. If you think might be looking at a piece of ROT13 code, all you need to do is to write the letters A-M on a piece of paper, and the letters N to Z below them. You can then substitute the letters accordingly, so if the cipher text has a letter A, the plain text is N and vice versa

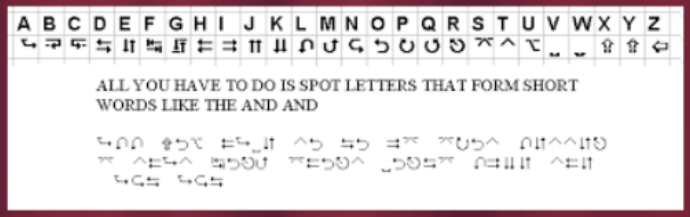
Prezi

Substitution Cipher

In cryptography, a substitution cipher is a method of encrypting in which units of plaintext are replaced with ciphertext, according to a fixed system; the "units" may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth.

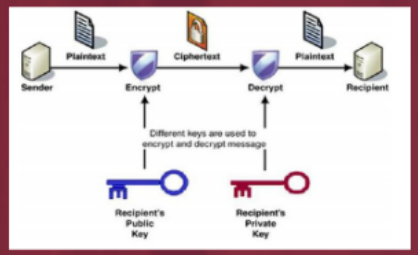
The mono-alphabetic cipher is subject to frequency attacks or guessing. The ciphertext has just as many 'A' characters as there are 'e' characters in the plaintext. Anyone trying to attack the ciphertext could use a table of the frequency of letters in the English language to make some smart guesses about which ciphertext characters are which plaintext characters. This succeeds relatively easily. Humans can do it, rather slowly, once they have about 10 words, sometimes less. This is a relatively common puzzle in newspapers, so it should not be surprising it's easy to break. Computers can also do it reliably when they have at least 150 characters.





Prezi

RSA algorithm



The RSA algorithm is an asymmetric cryptography algorithm; this means that it uses a public key and a private key (i.e two different, mathematically linked keys). As their names suggest, a public key is shared publicly, while a private key is secret and must not be shared with anyone.The RSA algorithm is named after those who invented it in 1978: Ron Rivest, Adi Shamir, and Leonard Adleman

RSA Algorithm

Key Generation

Select p,q	p and q both prime; $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n),e) = 1;\ 1 < e < \phi(n)$
Calculate d	$de \bmod \phi(n) = 1$
Public key	$KU = \{e,n\}$
Private key	$KR = \{d,n\}$

Encryption

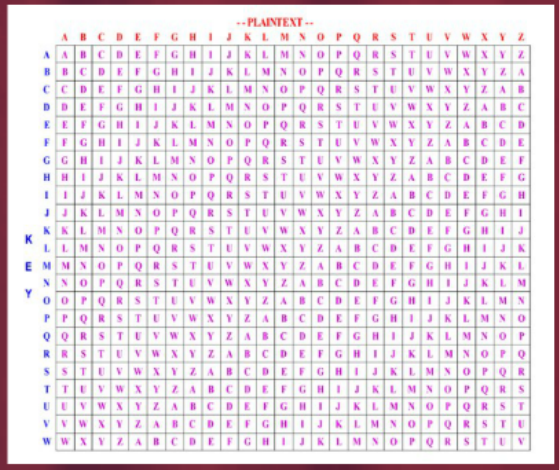
Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod n$

Decryption

Plaintext:	C
Ciphertext:	$M = C^d \pmod n$

Vigenere Cipher

One of the main problems with simple substitution ciphers is that they are so vulnerable to frequency analysis. Given a sufficiently large ciphertext, it can easily be broken by mapping the frequency of its letters to the know frequencies of, say, English text. Therefore, to make ciphers more secure, cryptographers have long been interested in developing enciphering techniques that are immune to frequency analysis. One of the most common approaches is to suppress the normal frequency data by using more than one alphabet to encrypt the message. A polyalphabetic substitution cipher involves the use of two or more cipher alphabets. Instead of there being a one-to-one relationship between each letter and its substitute, there is a one-to-many relationship between each letter and its substitutes.



Prezi

Playfair Cipher

In cryptosystems for manually encrypting units of plaintext made up of more than a single letter, only digraphs (pairs of letters) were ever used. By treating digraphs in the plaintext as units rather than as single letters, the extent to which the raw frequency distribution survives the encryption process can be lessened but not eliminated, as letter pairs are themselves highly correlated. The best-known digraph substitution cipher is the Playfair, invented in 1854 by Sir Charles Wheatstone but championed at the British Foreign Office by Lyon Playfair, the first Baron Playfair of St. Andrews

Secure Hashing algorithm

Secure Hash Algorithms (SHA) are used for computing a condensed representation of electronic data (message). When a message of any length less than 264 bits (for SHA-224 and SHA-256) or less than 2128 bits (for SHA-384, SHA-512, SHA-512/224 and SHA-512/256) is input to a hash algorithm, the result is an output called a message digest. Common names for the output of a hash function include also hash value, hash, and digital fingerprint. The SHA-3 hash functions can be implemented as alternatives to the SHA-2 functions, or vice versa.

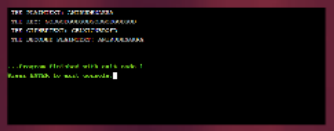
SHA-1 or Secure Hash Algorithm 1 is a cryptographic hash function which takes an input and produces a 160-bit (20-byte) hash value. This hash value is known as a message digest. This message digest is usually then rendered as a hexadecimal number which is 40 digits long. It is a U.S. Federal Information Processing Standard and was designed by the United States National Security Agency.

SHA-256 is one of the six variants of SHA family (SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256). These variants differ in size of their output, internal state size, block size, message size & rounds.
These days, all the major SSL Certificate issuers use SHA-256 which is more secure and trustworthy. Before SHA-1 was used, but it has been deprecated in January 2016, due to its security vulnerabilities it has become more susceptible to attacks and one of the reasons was a smaller bit size.

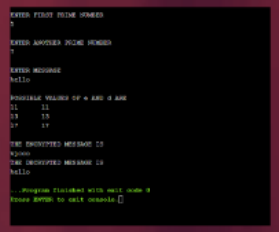
Prezi

Results

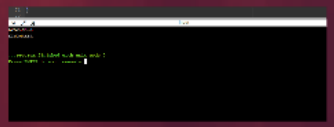
SHA256



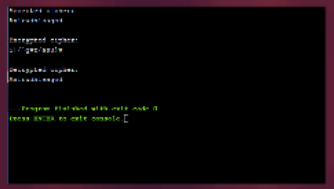
Vigenere



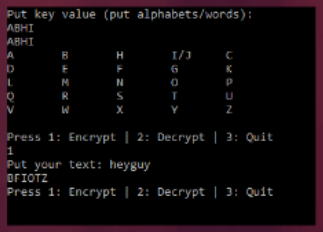
RSA



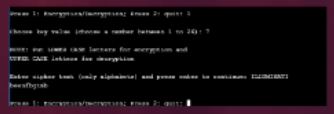
ROT13



XOR



Playfair



Caesar

Prezi

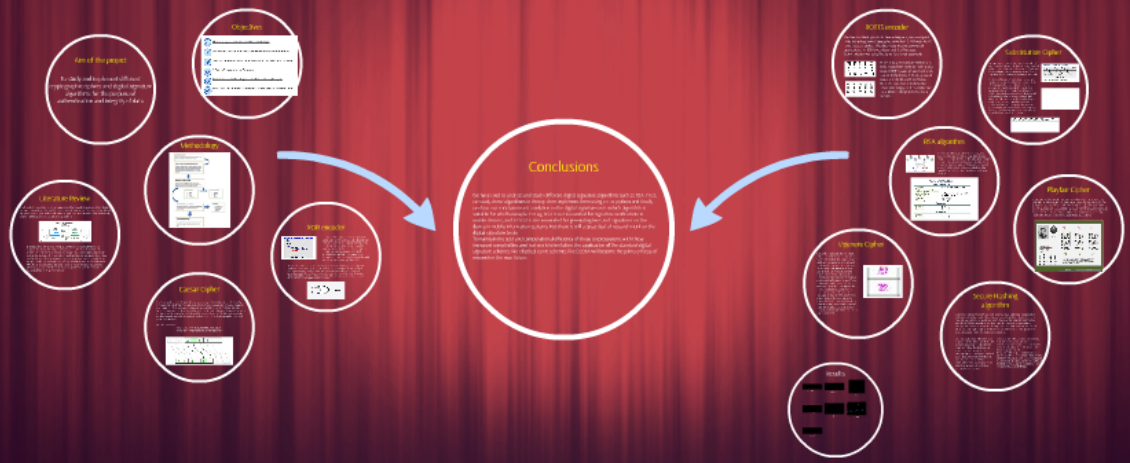
Conclusions

We have tried to analyze and study different digital signature algorithms such as RSA. First, we study these algorithms in theory, then implement them using c++ or python and finally, we draw our conclusions on a solution to the digital signature as to which algorithm is suitable for which example. For eg. RSA is recommended for signature verification on mobile devices, and ECDSA is recommended for generating keys and signatures on the device in mobile information systems. But there is still a great deal of research work on the digital signature to do.

To maintain the cost and computational efficiency of these cryptosystems with these increased complexities and real-world orientation, the application of the standard digital signature schemes like elliptical curve schemes like ECDSA will become the primary focus of research in the near future.

Prezi

Digital Signatures: Applications and Implementations



Prezi