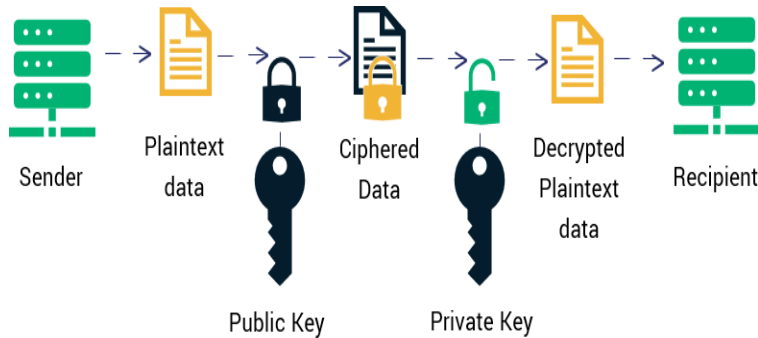
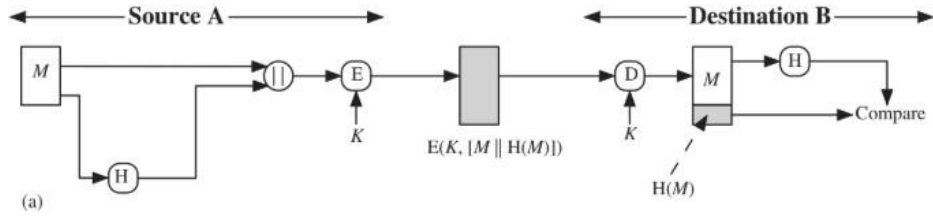
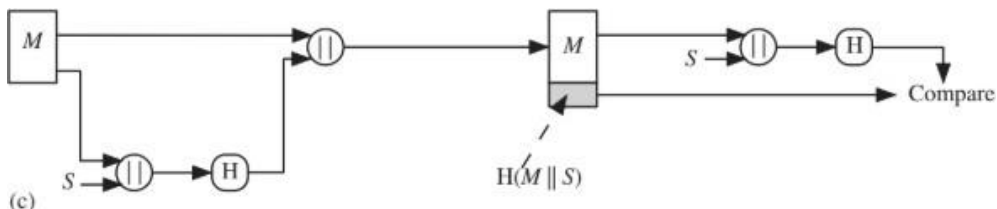
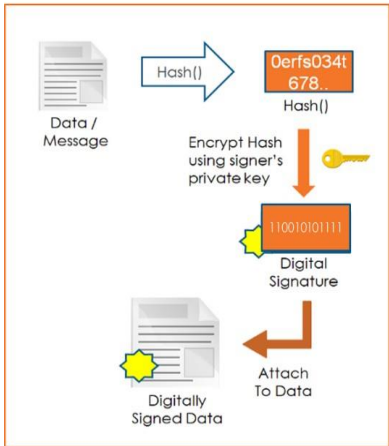
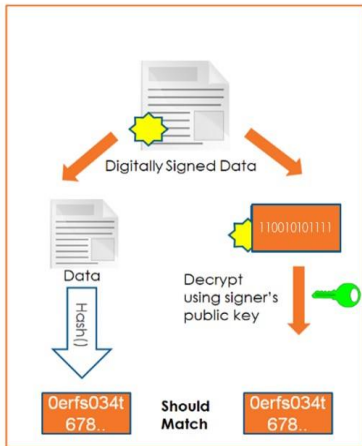


Charotar University of Science and Technology [CHARUSAT]**Chandubhai S. Patel Institute of Technology [CSPIT]****U & P U. Patel Department of Computer Engineering****Practical List**

Subject code	:	CE348	Semester	:	6	Academic Year	:	2020-21
Subject name	:	INFORMATION NETWORK SECURITY						

Sr. No.	Aim	Hrs.	CO
1.	Apply attacks for cryptanalysis to decrypt the original message from a given cipher text using Ceaser-Cipher and PlayFair cipher. Key = charusat	02	1,2,3
2.	Provide the extended version of Play-Fair cipher after launching Brute-Force attack in Practical-1. [Hint. Use extended matrix size which incorporates variety of symbols like alphabets, number, special symbol]	02	1,2,3
3.	Study and Configure Nmap (Network mapping tool) on Linux/Windows. Explore the various command for scanning your host/ips, ports and various services running on port. Prepare the document of at least 25 Nmap commands. Use the Nmap scrip and launch the DoS attack by flooding the packages in regular interval.	02	1,2,3,4
4.	The transmission of information need to be secure over the communication channel and the data has to be confidential. Study and implement the practical approach for Steganography. -Using DOS commands -Using OpenPuff Tool	02	1,2,3,4
5.	Bob is going to send his encrypted file using public key shared by Alice using Public-key infrastructure. Alice will decrypt the file by using her private key and ensure the confidentiality. Implement the following scenario using RSA algorithm. 	04	4,5

	After applying RSA, analyse the processing power of computer and speed with respective to time. Try using 1024 bit of key. Discuss what are the issues with this scenario.		
6.	<p>Refer to the figure (a) attached here. Bob (Source A) is preparing to send message to Alice (Destination B). Bob applies SHA256 hash algorithm on prepared message and append with original message (M) which is further encrypted by single secret key. Alice will receive bundle of encrypted $H(M)$ and original message (M). Alice will first apply single secret key to decrypt the entire bundle and collect $H(M)$ and original message (M). Furthermore, Alice will apply the same algorithm SHA256 which was used by Bob and produce hash of received message (H). Lastly, Alice will verify the computed hash with received $H(M)$ to make sure message is not altered by any attackers.</p>  <p>(a)</p> <p>Task to perform:</p> <ol style="list-style-type: none"> 1) Use any Symmetric key/Asymmetric key algorithm to implement encryption function and decryption. 2) Implementation can be done using any programming language such as c, c++, java, python, c#, javascript, etc. 3) For SHA256 hashing, you may use library compatible as per your programming language. <p>Discuss the issues causes with this scenario. What happened if we encrypt the generated hash?</p>	04	5
7.	<p>Refer to the attached figure here. Bob is preparing to send message to Alice. Bob and Alice both secretly computes the code(s) without sharing on any communication channel. Suggest key exchange algorithm to Bob and Alice for securely exchange information without sharing actual key. Once they form secret code, Bob applies SHA256 hash algorithm on original message (M) plus code (s) and send hash of original message and code ($M s$) to Alice. Alice will receive bundle of $H(M s)$ and first append code (s) with received message (M) and produce hash of the message (H) that compare with $H(M s)$ to make sure that message is not altered by any attackers.</p>  <p>(c)</p>	04	6

	<p>Task to perform:</p> <ol style="list-style-type: none"> 1. Use some key exchange algorithm to calculate value of s (secret code) which must be unique at sender and receiver side. 2. Implementation can be done using any programming language such as c, c++, java, python, c#, javascript, php etc. 3. Apply SHA256 on message and secret code and display it on output screen. Verify the hash value at receiver end. 		
8.	<p>A digital signature is a mathematical scheme for presenting the authenticity of digital messages or documents. A valid digital signature gives a recipient reason to believe that</p> <ul style="list-style-type: none"> • The message was created by a claimed sender (authentication), • The sender cannot deny having sent the message (non-repudiation), • The message was not altered in transit (integrity). <p>Practical Lab Set-up:</p> <div style="display: flex; justify-content: space-around;"> <div style="text-align: center;"> <p>1. Signing the message with Private Key</p>  </div> <div style="text-align: center;"> <p>2. Verifying the message with Public Key</p>  </div> </div> <p>Practically show the Digital Signature with context of Blockchain Technology or any other programming language and test the authenticity, non-repudiation, integrity of document (transaction).</p> <p>Reference: https://blockgeeks.com/what-is-hashing-digital-signature-in-the-blockchain/ https://medium.com/@xragrawal/digital-signature-from-blockchain-context-cedcd563eee5</p> 	04	5,6
9.	<p>System hacking is the way hackers get access to individual computers on a network. Ethical hackers learn system hacking to detect, prevent, and counter these types of attacks. Study practical approach to implement System Hacking and learn different ways to crack password.</p>	04	1-5
10.	<p>Attacking Web Application: SQL injection and Cross Site Scripting Attack</p>	02	1-5
11.	<p>Prepare the document along with presentation on latest security, privacy and integrity significance, issues (possible attacks) and their countermeasures. Show the demonstration by implementing any technology/algorithms/analysis using any</p>		1-6

	tools.		
--	--------	--	--

Prepared By:	Martin Parmar	Date:	
	Sneha Padhiar		