CSE2221 CRYPTOGRAPHY

CASE STUDY (10 MARKS)

VIDEO REPORT:

- **10 MARKS, MINIMUM DURATION 5 MINUTES, MAX 10 MINUTES**
- **VIDEO SHOULD HAVE THE PRESENTATION VISIBLE, WITH BOTH THE MEMBER'S FACE VISIBLE WITH CLEAR AUDIO**
- **THERE SHOULD NOT BE ANY GLITCH IN THE VIDEO, OTHERWISE RELEVANT MARKS WILL BE CUT**

REPORT

- **10 PAGES PLAG AND AI FREE CONTENT**
- **EQUAL CONTRIBUTION BY BOTH MEMBERS SHOULD BE CLEARLY MENTIONED**
- **HEADER WITH 12 FONT AND TEXT BODY AS 10 FONT, TIMES NEW ROMAN, DEFAULT PAGE, LINE AND PARAGRAPH SPACING WITH NO ABNORMALITIES**

You will be allotted one algorithm from the following table and one case study from the following given case studies. You must make a video presentation on the both the topics, and a plag and AI free report on the same. Both the members should have equal contribution in all the aspects. You must work in a team of 2. Submissions will be done on teams in the form of assignments. You may upload the video report in a google/OneDrive link. Report should be 10 pages minimum, with 5 pages for each topic.

1. **Real-world Case Studies**: Students must research real-world instances where these algorithms have been used or attacked. This will give them a practical understanding of how these algorithms function in the real world. You may select any of the case studies attached in the documents or you may also select some relevant attacks as well.
2. **Implementation**: Additional marks may be given if implementation of a simple version of one of these algorithms is done. This would give them hands-on experience and a deeper understanding of the algorithm.
3. **Presentation**: Students are asked to present their findings to the class/video presentation, explaining the algorithm/attacks they researched, its uses, any known attacks, and their own implementation.

Instructions:

- **OneDrive/Google Drive link should be working otherwise relevant marks will be cut**
- **Video should be properly made with audio from both members, otherwise ZERO marks will be given.**
- **Report should be plag/AI free as it will be run through Turnitin software, if any plag/AI found ZERO marks will be awarded.**

A list of some post-quantum cryptographic algorithms and their resources:

Serial Number	Algorithm Name	Resource
1	Lattice-based cryptography	Wikipedia
2	Learning with errors (LWE)	Wikipedia
3	Ring learning with errors (ring-LWE)	Wikipedia
4	NTRU encryption schemes	Wikipedia
5	NTRU signature and BLISS signatures	Wikipedia
6	Lattice-based cryptography	NIST PQC
7	Learning with errors (LWE)	NIST PQC
8	Ring learning with errors (ring-LWE)	NIST PQC
9	NTRU encryption schemes	NIST PQC
10	NTRU signature and BLISS signatures	NIST PQC
11	CRYSTALS-Dilithium	NIST PQC
12	CRYSTALS-KYBER	NIST PQC
13	SPHINCS+	NIST PQC

SNO	Algorithm	Type	Public Key	Private Key	Signature
14	NTRU Encrypt[42]	Lattice	766.25 B	842.875 B	

SNO	Algorithm	Type	Public Key	Private Key	Signature
15	Streamlined NTRU Prime[citation needed]	Lattice	154 B		
16	Rainbow[43]	Multivariate	124 KB	95 KB	
17	SPHINCS[23]	Hash Signature	1 KB	1 KB	41 KB
18	SPHINCS+[44]	Hash Signature	32 B	64 B	8 KB
19	BLISS-II	Lattice	7 KB	2 KB	5 KB
20	GLP-Variant GLYPH Signature[14][45]	Ring-LWE	2 KB	0.4 KB	1.8 KB
21	NewHope[46]	Ring-LWE	2 KB	2 KB	
22	Goppa-based McEliece[18]	Code-based	1 MB	11.5 KB	
23	Random Linear Code based encryption[47]	RLCE	115 KB	3 KB	
24	Quasi-cyclic MDPC-based McEliece[48]	Code-based	1,232 B	2,464 B	
25	SIDH[49]	Isogeny	564 B	48 B	
26	SIDH (compressed keys)[50]	Isogeny	330 B	48 B	

27	3072-bit Discrete Log	**not PQC**	384 B	32 B	96 B
28	256-bit Elliptic Curve	**not PQC**	32 B	32 B	65 B

1. Diffie-Hellman:

- The Diffie-Hellman Key Agreement Protocol allows use of long exponents that arguably make certain calculations unnecessarily expensive[20].
- The Logjam Attack on TLS connections using the Diffie-Hellman (DH) key exchange protocol affects IBM® WebSphere Real Time[21].

2. Elliptic Curve:

- Researchers have demonstrated how existing attacks against the ECDSA cryptographic algorithm can be improved to reduce the required nonce leakage by exploiting side-channel vulnerabilities[1].
- The Elliptic Curve Digital Signature Algorithm (ECDSA) is vulnerable to LadderLeak, a side-channel attack[1].

3. Double DES:

- Double DES is susceptible to meet-in-the-middle attacks, where two different inputs produce the same hash[19].
- Double DES uses 112-bit key but gives security level of 2^56 not 2^112 due to meet-in-the-middle attack[19].

4. Advanced AES:

- AES is vulnerable to brute force attack and Man-in-the-Middle (MITM) attack[14].
- Far field electromagnetic (EM) emission as a side channel has been used to attack AES[13].

5. SHA-1:

- SHA-1 is susceptible to collision attacks, where two different inputs produce the same hash[78].

- Preimage attacks can reverse-engineer the hash to find an input that matches a given SHA-1 hash, compromising data security[7].

6. MD5:

- MD5 is susceptible to collision attacks, where two different inputs produce the same hash[13].

- Preimage attacks can reverse-engineer the hash to find an input that matches a given MD5 hash, compromising data security[13].

7. SHA-256:

- SHA-256 is part of the SHA-2 family of hash functions and uses a 256bit key to take a piece of data and convert it into a new, unrecognizable data string of a fixed length[11].

- The Merkle–Damgård architecture is used in SHA-256 and is vulnerable to length extension attacks[12].

Source(s)

1. NVD - CVE-2022-40735
2. Security Bulletin: Vulnerability in Diffie-Hellman ciphers ... - IBM 3. LadderLeak: Side-channel security flaws exploited to break ECDSA ...
4. meet in the middle attack - 2Des is double secure of DES ...
5. hash - Why is MD5 considered a vulnerable algorithm? - Information ...
6. Exploring the Power and Vulnerabilities of the MD5 Algorithm
7. NIST retires SHA-1 cryptographic algorithm due to vulnerabilities
8. NIST Retires SHA-1 Cryptographic Algorithm | NIST
9. SHA 256 Algorithm Explained by a Cyber Security Consultant
10. A comprehensive review of the security flaws of hashing algorithms ...
11. On the Attacks over the Elliptic Curve-Based Cryptosystems
12. Examining CVE-2020-0601 Crypt32.dll Elliptic Curve Cryptography (ECC ...
13. Review of the Advanced Encryption Standard - NIST
14. Advanced Encryption Standard: Attacks and Current Research Trends
15. AES Vulnerabilities Study | IEEE Conference Publication - IEEE Xplore
16. SHA1 Collision Signals the End of the Algorithm's Viability
17. SHA256 security: what does it mean that attacks have broken "46 of the ...
18. Patching the Perpetual MD5 Vulnerability | Venafi
19. MD5 Collision Vulnerability: Generating Identical Hash Values From Two ...
20. Double DES and Triple DES - GeeksforGeeks
21. Data Encryption Standard - Wikipedia
22. Is there a complete summarized list of attacks on Diffie-Hellman?
23. https://dheatattack.gitlab.io/
24. https://gist.github.com/c0r0n3r/9455ddcab985c50fd1912eabf26e058b
25. https://github.com/mozilla/ssl-config-generator/issues/162
26. https://link.springer.com/content/pdf/10.1007/3-540-68339-9_29.pdf 27. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf
28.

https://raw.githubusercontent.com/CVEProject/cvelist/9d7fbbcabd3f44cfedc9e8807757d31ece85a2c6/2022/40xxx/CVE-2022-40735.json
29. https://exchange.xforce.ibmcloud.com/vulnerabilities/103294
30. https://ieeexplore.ieee.org/servlet/opac?punumber=6353658 31. https://doi.org/10.6028/NIST.IR.8319
32. https://ieeexplore.ieee.org/servlet/opac?punumber=9404366
33. https://crypto.stackexchange.com/questions/1434/are-there-two-known-strings-which-have-thesame-md5-hash-value

1. RSA:

- RSA SecurID, a multi-factor authentication technology, has certain vulnerabilities. If a perpetrator successfully steals a token, card, or badge, they will have access to one of the two steps for authentication[1].
- There are also attacks like plain text attacks, chosen cipher attack, factorization attack, and attacks on encryption and decryption keys[2].
- A reduced-strength variant of RSA was found to be vulnerable to attacks[4].
- Power analysis and timing attacks are the two most common sidechannel attacks on RSA encryption[3].

2. ElGamal:

- The ElGamal implementation in Crypto++ through 8.5 allows plaintext recovery because of a dangerous combination of the prime defined by the receiver's public key, the generator defined by the receiver's public key, and the sender's ephemeral exponents[9].
- The ElGamal implementation in Libgcrypt before 1.9.4 has similar vulnerabilities[10].

3. AES:

- AES is vulnerable to brute force attack and Man-in-the-Middle (MITM) attack[14].
- Far field electromagnetic (EM) emission as a side channel has been used to attack AES[13].

4. DES:

- DES has been considered insecure right from the start because of the feasibility of brute-force attacks[6].
- It has fallen out of use due to technological developments making it an increasingly insecure encryption method[7].

Please note that while these algorithms have had vulnerabilities, they have also been instrumental in the advancement of cryptography and have formed the basis for more secure algorithms. It's also important to remember that no

encryption method is completely foolproof, and the security of an encryption method often depends on how it's implemented and used.

Source(s)

1. What Is RSA SecurID? Common Vulnerabilities and How It Works - Fortinet 2. Security of RSA - GeeksforGeeks
3. One in every 172 active RSA certificates are vulnerable to attack
4. RSA Algorithm in Cryptography: Rivest Shamir Adleman Explained
5. NVD - CVE-2021-40530
6. NVD - CVE-2021-40528
7. web application - Is AES encryption vulnerable? - Information Security ...
8. Advanced Far Field EM Side-Channel Attack on AES - KTH
9. Data Encryption Standard - Wikipedia
10. What Is DES Encryption? A Look at the DES Algorithm
11. How Secure is RSA in an Increasingly Connected World?
12. NIST Identifies Types of Cyberattacks That Manipulate Behavior of AI ...
13. Fault Attacks on ElGamal-Type Cryptosystems - uni-passau.de
14. Review of the Advanced Encryption Standard - NIST
15. Cryptography-based Vulnerabilities in Applications | Infosec
16. Finding the Keys to the Kingdom: Researchers Devise an Attack on the ...
17. https://eprint.iacr.org/2021/923
18. https://ibm.github.io/system-security-research-updates/2021/07/20/insecurity-elgamal-pt1
19. https://ibm.github.io/system-security-research-updates/2021/09/06/insecurity-elgamal-pt2 20. https://lists.fedoraproject.org/archives/list/packageannounce%40lists.fedoraproject.org/message/57OJA2K5AHX5HAU2QBDRWLGIIUX7GASC/
21. https://lists.fedoraproject.org/archives/list/packageannounce%40lists.fedoraproject.org/message/HGVBZ2TTRKCTYAZTRHTF6OBD4W37F5MT/
22. https://lists.fedoraproject.org/archives/list/packageannounce%40lists.fedoraproject.org/message/VJYOZGWI7TD27SEXILSM6VUTPPEICDL7/
23. https://doi.org/10.6028/NIST.IR.8319
24. https://doi.org/10.1145/3457339.3457982