Assignment 4: ABCs of Digital Certificates

Individual Assignment

PART-A: Comparison of Digital Certificates in the chain of trust of a popular website

- Visit the website <mark>#N</mark> in <u>this list of top-100 most visited websites globally</u> where is <mark>#N is the last two digits in your roll number</mark> and download all the certificates in .CER or .PEM format in the chain of trust from the root Certificate, intermediate certificate(s), to the end-user (website) certificate at the leaf in the hierarchy.
- Compare the digital certificates in the chain in terms of various field values by filling this table.

Field Name	Subject (CN) of certificate holder (website)	Subject (CN) of certificate holder (intermediate)	Subject (CN) of certificate holder (intermediate, if applicable)	Subject (CN) of certificate holder (root)	Remarks/observations
Issuer					
Version No.					
Signature Algo					
Size of digest that is signed to generate Cert Sign					
Size of Cert Signature					
Validity period					
Is Subject field (CN), FQDN?					
Certificate type: DV, IV, OV or EV?					

Tell also how you are able to determine the type!					
Subject Alternative Name(s) (SAN/UCC), if any					
Certificate category: Single domain, wildcard, Multi-domain SAN/UCC cert?					
Public Key Info like key algo, key length, public exponent (e) in case of RSA					
Public key or modulus (n) in case of RSA					
Key usages; how do they vary in the chain, mention in the remarks?					
Basic constraints, how do they vary in the chain?					
Name constraints					

(if any), how are these useful?					
Size of the certificate					
URI of CRL					
URI of OCSP Responder					
Any other parameters that you found interesting?					

Answer the following queries after filling out the above table:
1. Which certificate type (DV/OV/IV/EV) is more trustable, secure, and expensive?
2. What is the role of the Subject Alternative Name (SAN) field in X.509 certificates?
3. Why are key usages and basic constraints different for root, intermediate and end certificates? What could go wrong if all of them have the same values?
4. What is the difference between Signature value and Thumbprint aka Fingerprint of a digital certificate?
5. Why do RSA key lengths increase over the years? Why is ECDSA being preferred over RSA now-a-days?
6. What are pros and cons of pre-loading root and intermediate certificates in the root stores of browsers and OSes?
7. Why are root CAs kept offline? How do they issue certificates to intermediate CAs?
8. Why are root and intermediate certificates of new CAs cross-signed by the legacy CAs? Answer this by taking Let's Encrypt and its parent organization as root and intermediate CAs.
9. What challenge is posed to the certificate seekers (Alice) by Let's Encrypt CA before issuing wildcard certificates? How does Alice respond to it so that she passes it?
10. List out names of OS/Browser/Company whose root stores were pre-populated with Root and Intermediate CA certificates of the website #N?

PART-B

1. A browser X has received the digital certificate of the website #N over a TLS connection. How does it verify whether the certificate is valid? Write a psuedo-code of browser X's verifier function named myCertVerifier( ) and explain how it works by picking the entire

chain of trust of an end-user cert (of the website **#N**) in PART-A of this assignment.

2. Consider the scenario in which evil Trudy has used the domain validated (DV) digital certificate of the website **(Bob) named Bob.com** to launch her own web server with the domain name, **xyz.com**. Does your function myCertVerify( ) returns valid or invalid for this when someone like Alice (browser) tries to access Trudy's website xyz.com?

3. Consider another scenario in which evil Trudy has used the digital certificate of Bob's website **Bob.com** to launch her own web server with the domain name, **xyz.com**. When a web client (Alice) tries to connect with Bob's website by sending a DNS query, Trudy responds with her IP address by DNS cache poisoning (What is DNS cache poisoning? | DNS spoofing | Cloudflare) Does your function myCertVerifier( ) returns valid or invalid for this and what are the consequences? What kind of attacks can Trudy launch in this scenario?

Deliverables in GC:

● Certificates used for completing this assignment and a readable PDF Report with name "Asg4-<RollNo>.PDF" compressed and encrypted with AES-256 using open source 7-zip file archiver tool with your RollNo (UPPERCASE) as the password.
  ○ In your report, briefly explain how 7-zip uses the password to encrypt compressed files using secure hash and symmetric algorithms. What role does the password length play in brute force attacks to decrypt the encrypted files?

References:
1. **https://crt.sh/**
2. **https://ahrefs.com/blog/most-visited-websites/**
3. **http://lapo.it/asn1js/#**
4. **http://phpseclib.sourceforge.net/x509/decoder.php**
5. **https://www.ssl.com/article/dv-ov-and-ev-certificates/**
6. **https://www.ccadb.org/**
7. **DV, OV, IV, and EV Certificates - SSL.com**
8. **7-Zip (7-zip.org)**

PLAGIARISM STATEMENT <Include it in your report>

I certify that this assignment/report is my own work, based on my personal study and/or research and that I have acknowledged all material and sources used in its preparation, whether they be books, articles, reports, lecture notes, and any other kind of document, electronic or personal communication. I also certify that this assignment/report has not previously been submitted for

assessment in any other course, except where specific permission has been granted from all course instructors involved, or at any other time in this course, and that I have not copied in part or whole or otherwise plagiarized the work of other students and/or persons. I pledge to uphold the principles of honesty and responsibility at CSE@IITH. In addition, I understand my responsibility to report honor violations by other students if I become aware of it.

Name:
Date:
Signature: <keep your initials here>

Late Policy:

10% cut in marks for each late day