Assignment 1: ABCs of Digital Certificates

Individual Assignment

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

- Visit the website #N in this list of top-100 most visited websites where is #N is the last two digits in your roll number and download all the certificates in .CER 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 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					
Signature Value					
Validity period					
Subject (CN)					
Certificate type: DV, IV, OV or EV? Tell also how you are able to determine the type!					
Subject					

Alternative Name (SAN), if any					
Certificate category: Single domain, wildcard or 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					
Basic constraints					
Name constraints, how these are useful?					
Size of the certificate					
Any other parameter?					

Answer the following queries after filling out the above table:

1. Which certificate type (DV/OV/IV/EV) is more trustable and expensive?
2. What is the role of Subject Alternative Name (SAN) field?
3. Why are key usages and basic constraints different for root, intermediate and end certificates?
4. Why do RSA key lengths increase over the years? Why ECDSA is being preferred over RSA now-a-days?

5. What are pros and cons of pre-loading root and intermediate certificates in the root stores of browsers and OSes?
6. Why are root CAs kept offline?

PART-B

1. You have received a digital certificate of a firm M over email. How do you verify whether the certificate is valid without using any of online tools or browsers? Write a psuedo-code of your verifier function named myCertChecker( ) and explain how it works by picking the chain of trust of an end-user cert in PART-A of this assignment.

2. Consider the scenario in which evil Trudy has used the digital certificate of firm M to launch her own web server. Does your function myCertChecker( ) returns valid or invalid for this when someone tries to access Trudy's website from a browser like Chrome/Edge/Firefox?

Deliverables in GC:

- Certificates used for completing this assignment and a readable PDF Report with name "DCAsg-<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, also briefly explain how 7-zip uses the password to encrypt compressed files using secure hash and symmetric algorithms. What role password length plays 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. 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 plagiarised 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 honour 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