National Taiwan Normal University
CSIE Information Security

Instructor: Po-Wen Chi
Due Date: May 13, 2024, PM 11:59

Assignment 3

Policies:

- Zero tolerance for late submission.
- Please pack all your submissions in one zip file. **RAR is not allowed!!**
- I only accept **PDF**. MS Word is not allowed.
- Hand-writing is not allowed.
- Please use **Chinese.**

3.1 Equivalent Assumptions (20 pts)

Consider a specific cyclic group $\mathbb{G}$ of prime order q generated by $g \in \mathbb{G}$. Show that the following problems are deterministic poly-time equivalent:

- Given g^α, g^β, compute $g^{\alpha\beta}$.
- Given g^α, compute g^{α^2}.
- Given g^α and $\alpha \neq 0$, compute $g^{\frac{1}{\alpha}}$.
- Given g^α, g^β with $\beta \neq 0$, compute $g^{\frac{\alpha}{\beta}}$.

Note that all problem instances are defined with respect to the same group $\mathbb{G}$ and generator $g \in \mathbb{G}$.

3.2 Implicit certificate (15 pts)

In this class, I have shown you how PKI works. Now I want to introduce a new technique called **implicit certificate**. In the traditional PKI system, the user public key is embedded in the certificate and the certificate is signed by a trusted authority. In cryptography, implicit certificates are a variant of public key certificate, where the public key is reconstructed, **not contained**, from the data in an implicit certificate. Tampering with the certificate will result in the reconstructed public key being invalid. Therefore, the implicit is generally smaller than the traditional certificate.

The scheme is as follows:

- **CA**:
  - A group $\mathbb{G}$ of order n with a generator G.
  - The private key is c and the public key is $Q_{CA} = cG$.
- **Certificate Request Protocol**:
  1. Alice generates a random number α and sends αG to CA.
  2. CA picks a random number k and computes kG.
  3. CA computes $\gamma = \alpha G + kG$.
  4. CA computes **Cert**= **Encode**(γ, ID_A).
  5. CA computes $e = H(\textbf{Cert})$.
  6. CA computes $s = ek + c$.
  7. CA sends $(\textbf{Cert}, s)$ to Alice.
  8. Alice computes $e' = H(\textbf{Cert})$ and her private key is $a = e'\alpha + s$.
  9. Alice derives $\gamma' = \textbf{Decode}(\textbf{Cert})$ and her public key is $Q_A = e'\gamma' + Q_{CA}$
- **Using the Certificate**:
  1. Alice sends **Cert** to Bob.
  2. Bob computes $e'' = H(\textbf{Cert})$ and $\gamma'' = \textbf{Decode}(\textbf{Cert})$.
  3. Bob computes Alice's public key $Q''_A = e'\gamma'' + Q_{CA}$.

Please show

1. The equivalence of Alice's private and public keys. That is, prove $Q_A = aG$.
2. Please show that given CA's public key Q_{CA}, without the CA secret key c, it is computationally infeasible to generate a valid certificate. The certificate is valid if $Q_A = aG$.

3.3 SoftEther (25 pts)

SoftEther VPN is free open-source, cross-platform, multi-protocol VPN client and VPN server software, developed as part of Daiyuu Nobori's master's thesis research at the University of Tsukuba.

https://github.com/SoftEtherVPN/SoftEtherVPN

Please write a tutorial with screen captures to teach me how to use it.

3.4 Random Number Generator in Linux Kernel (10 pts)

I have told you that Linux kernel change its pseudo-random device behavior. Please read the following material.

https://lwn.net/Articles/884875/

I told you that I want to submit a patch to SEED lab. So please help me to find the commit of this change and show that **/dev/random** and **/dev/urandom** are now the same thing.

3.5 Lab: MD5 Collision Attack Lab (15 pts)

- Lab: https://seedsecuritylabs.org/Labs_20.04/Crypto/Crypto_MD5_Collision/

You need to submit a detailed lab report, with screenshots, to describe what you have done and what you have observed. You also need to provide explanation to the observations that are interesting or surprising. Please also list the important code snippets followed by explanation. Simply attaching code without any explanation will not receive credits.

3.6 Lab: PKI Lab (15 pts)

- Lab: https://seedsecuritylabs.org/Labs_20.04/Crypto/Crypto_PKI/

You need to submit a detailed lab report, with screenshots, to describe what you have done and what you have observed. You also need to provide explanation to the observations that are interesting or surprising. Please also list the important code snippets followed by explanation. Simply attaching code without any explanation will not receive credits.