Authors: Aadi Akyianu, Lazuli Kleinhans

Cryptographic Scenarios Questions

1. **Alice wants to send Bob a long message, and she doesn't want Eve to be able to read it. Assume for this scenario that AITM is impossible.**
    - Use Diffie Helman to determine a shared key, K
    - Use `K` in `AES` to such that `C = AES(K, M)` where `M` is the message that Alice wants to send to Bob.
    - Send `C` to Bob and he can decrypt it using `AES_D(K, C) = M`
    - `(P, S)`

2. **Alice wants to send Bob a long message. She doesn't want Mal to be able to modify the message without Bob detecting the change.**
    - Alice should use a public/secret key pair `(P_A, S_A)`. She should share `P_A` with Bob and keep `S_A` completely secret.
    - Similarly, Bob should also have his own `(P_B, S_B)`. He should share `P_B` with Alice.
    - From there they can encrypt their messages and use Diffie Helman to determine a shared key, `K`
    - Use `K` in `AES` to such that `C = AES(K, M)` where `M` is the message that Alice wants to send to Bob.
    - Calculate `H(M)` and concatenate that with `C`.
    - Send `C||H(M)` to Bob and he can decrypt it using `AES_D(K, C) = M’`.
    - Then he can check that Mal did not interfere by making sure that `H(M’) = H(M)`

3. **Alice wants to send Bob a long message (in this case, it's a signed contract between AliceCom and BobCom), she doesn't want Eve to be able to read it, and she wants Bob to have confidence that it was Alice who sent the message. Assume for this scenario that AITM is impossible**
    - Use Diffie Helman to determine a shared key, `K`

- Use `K` in `AES` to such that `C = AES(K, M)` where `M` is the message that Alice wants to send to Bob.
- Alice should create a public/secret key pair `(P_A, S_A)`. She should share `P_A` with Bob and keep `S_A` completely secret.
- Similarly, Bob should also have his own `(P_B, S_B)`. He should share `P_B` with Alice.
- To prove that this message came from Alice, she should encrypt a hash of the message `H(M)` with her private key, calculating `E(S_A, H(M))`.
- To ensure that only Bob can read the message, she should then encrypt it with Bob's public key `P_B`, using `E(P_B, E(S_A, H(M)))` to get `X`.
- Alice should then send `C||X` to Bob.
- Bob can get `M` with `AES_D(K, C)`, and then verify that it truly did come from Alice by calculating `E(P_A, E(S_B, X))` to get `H(M)'` and making sure that `H(M)' = H(M)`.

4. Consider a scenario where Alice and Bob have been in contract negotiations and sharing documents electronically along the way. Suppose Bob sues Alice for breach of contract and presents as evidence the digitally signed contract `(C || Sig)` and Alice's public key `P_A`. Here, `C` contains some indication that Alice has agreed to the contract—e.g., if `C` is a PDF file containing an image of Alice's handwritten signature. `Sig`, on the other hand, is a digital signature.

   Suppose Alice says in court "`C` is not the contract I sent to Bob". (This is known as *repudiation* in cryptographic vocabulary.) Alice will now need to explain to the court what she believes happened that enabled Bob to end up with an erroneous contract. List at least three things Alice could claim happened. For each of Alice's claims, state briefly how plausible you would find the claim if you were the judge. (Assume that you, the judge, studied cryptography in college.)

   - Alice could claim that an AITM replaced `C` with some `C'`

Authors: Aadi Akyianu, Lazuli Kleinhans

  - not plausible because we could confirm by taking `H(C)` and calculating `E(S_A, Sig)` and if the two are the same then C was not replaced.
- Alice could claim that `P_A` is not her public key. That is, someone else was pretending to be Alice to Bob:
  - This could be plausible considering there was no Certificate Authority used to verify that `P_A` belongs to Alice
- Alice could claim that her secret key was stolen and used by an adversary to send a counterfeit contract to Bob.
  - This could also be possible as, although she is supposed to keep her secret key private, if someone else got their hands on it, they could encrypt messages to Bob that would seem authentic.

5. For this scenario, suppose the assumption that everybody has everybody else's correct public keys is no longer true. Instead, suppose we now have a certificate authority CA, and that everybody has the correct `P_CA` (i.e. the certificate authority's key). Suppose further that Bob sent his public key `P_B` to CA, and that CA then delivered to Bob this certificate:

```
Unset
Cert_B = "bob.com" || P_B || Sig_CA
```

   In terms of `P_CA`, `S_CA`, `H`, `E`, etc., what would `Sig_CA` consist of? That is, show the formula CA would use to compute `Sig_CA`.
   - `Sig_CA = E(S_CA, H(M))` where `M = "bob.com" || P_B`

6. Bob now has the certificate `Cert_B` from the previous question. During a communication, Bob sends Alice `Cert_B`. Is that enough for Alice to believe she's talking to Bob? (Hint: no.) What could Alice and Bob do to convince Alice that Bob has the `S_B` that goes with the `P_B` in `Cert_B`?
   - Alice should run the following steps to verify the certificate:

    - First Alice would extract `Sig_CA` from the rest of the data in `Cert_B`. (We are assuming `Cert_B` utilized the `SHA-256` hash function meaning `Sig_CA` is the last 64 hex digits of the message)
    - Next Alice would calculate `H(X)` where `X` denotes the data extracted from `Cert_B`.
    - Afterwards she would compute `E(P_CA, Sig_CA)` and compare this value to `H(X)`. If the two are the same then the certificate is legitimate.
    - This means that she can trust that `bob.com` is associated with `P_B`.
  - Bob would then send a message to Alice that is encrypted with `S_B` and if Alice can encrypt it with `P_B`, then she knows that Bob has the `S_B` that goes with `P_B`.

7. Finally, list at least two ways the certificate-based trust system from the previous two questions could be subverted, allowing Mal to convince Alice that Mal is Bob.
   - If Alice's browser has the wrong `P_CA` and instead has Mal's public key
   - If Mal hacks the CA and produces a signature that states their own malicious website is the real Bob.