Network Security and Cryptography

Summative Assessment 2

Submission Deadline 5 December Thursday 9.59 AM UK time

Question 1

Consider the following RSA based signature scheme that we will call BadSign. H is a hash function mapping onto $\mathbb{Z}_n^*$. Set $\lambda = 1024$.

```
Procedure Keygen($1^\lambda$)
    Choose two random $\lambda/2$-bit primes $p$ and $q$
    Choose a hash function $H\colon \{0,1\}^* \to \mathbb{Z}_n^*$
    $n = p \cdot q$
    $\phi = (p-1)(q-1)$
    Select $e$ such that
        $1 < e < \phi$ and $\gcd(e, \phi) = 1$
    Compute $d$ such that
        $1 < d < \phi$ and $ed \equiv 1 \pmod{\phi}$
    Set $PK = (e, n, H)$
    Set $SK = (d)$
    return $(PK, SK)$
```

```
Procedure Sign($SK, m$)
    $r \xleftarrow{\$} \mathbb{Z}_n^*$
    $\sigma_1 = H(m)^d r^d \bmod n$
    $\sigma = (\sigma_1, r)$
    return $\sigma$
```

1. Write a verification algorithm for the signature scheme.

   [2 points]

2. Show that BadSign is not secure.

   [4 points]

Question 2

We claim that the randomness reuse in DSA is unsafe. Suppose, the same random $r \in \mathbb{Z}_q^\times$ is used to create a signature (s_1, t_1) on message M_1, and a signature (s_2, t_2) on message M_2. Show that an adversary could recover the secret signing key from the signatures and the messages.

[4 pts]

Question 3

Alice and Bob own a shared bank account, and, unfortunately, Bob cannot remember the four-digit PIN to access the account. Alice wants to help her partner Bob and send him the PIN via an end-to-end encrypted messenger.

The messenger they use provides end-to-end encryption based on the Wired Equivalent Privacy (WEP) protocol and a short out-of-band shared secret. The shared secret Alice and Bob agreed to is a **4 letter word** (subsequently denoted *key*), consisting only of the following 26 symbols:

`abcdefghijklmnopqrstuvwxyz`

Let $z \leftarrow\!\!\$\ Z$ denote a random integer $z \in Z$.

Let $m \leftarrow$ "`Our secret PIN code is: XXXX`" be the message Alice wants to send to Bob. The message is assumed to be ASCII encoded[1], representing each letter/digit as one byte.

Alice		**Bob**
$IV \leftarrow\!\!\$\ \{0, 1, \dots, 2^{64}\}$		
$\mathit{keystream} \leftarrow \mathit{RC}4(IV \mid\mid \mathit{key})$		
$c \leftarrow m \oplus \mathit{keystream}$		
	$\xrightarrow{IV, c}$	
		$\mathit{keystream} \leftarrow \mathit{RC}4(IV \mid\mid \mathit{key})$
		$m \leftarrow c \oplus \mathit{keystream}$

The protocol essentially consists of a one-time pad encryption using the beginning of *keystream* as key.

1. Does the above protocol guarantee *confidentiality*, *data integrity*, and *authentication*? For each property, justify your answer and give an attack on the property if possible.

   [6 pts]

2. Assume the adversary got hold of

   $$\begin{aligned} IV &= \texttt{0xd459caface298bbb} \\ c &= \texttt{0x0cfd567edc556b86ec2fe5ed73f302cc} \\ &\ \texttt{71816605e19898eff837172a} \end{aligned}$$

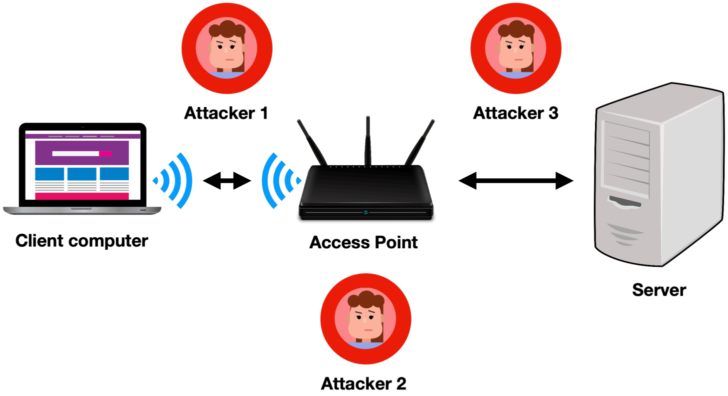
   Recover the plaintext PIN and give the shared secret *key*. You will have to write a small computer program to assist you in your task.

   [4 pts]

[1] Encoding tables can be found online, e.g., `https://www.ascii-code.com`.

Question 4

Assume a setup as shown below. A client computer is connected to a wireless access point and from there via a wired network to a server. The client wishes to download an important document from the server.



For this question, we consider three different attackers. Attacker 1 is located in between the client and the access point and can listen to the wireless network traffic. Attacker 2 is located on the access point. Attacker 3 is located in between the access point and the server.

For each attacker, consider the following three scenarios and explain whether confidentiality and integrity of the document is achieved? If not, explain how the attacker might be able to read or modify the document.

1. The client uses a secure WPA3 connection with the AP. There is no TLS connection between the client and the server.
2. The client uses a WEP connection with the AP. There is no TLS connection between the client and the server.
3. The client uses a WEP connection with the AP. There is a secure TLS connection between the client and the server.

[6 pts]

Question 5

Certificate pinning is the process of tying a host to their expected X.509 certificate. This can be done at development time of an application by requiring that the certificate of a TLS connection be a member of a prespecified set. You can see an example of certificate pinning in pseudo-code below:

```
function onConnect(connection, certificate):
    if hash(certificate) == '098f6bcd4621d373cade4e832627b4f6':
        return true
    connection.close()
    return false  # abort the connection
```

Explain why it is useful to use certificate pinning when using self-signed certificates. Also describe what kinds of attacks are mitigated by this practice?

[4 pts]