
1. Suppose naive Nelson tries to implement the following three pass protocol to send a key $K$ to Heidi. He chooses a one-time pad key $K_N$ and XORs it with $K$. He sends $M_1 = K_N \oplus K$ to Heidi. She XORs what she receives with her one-time pad key $K_H$ to get $M_2 = K_H \oplus M_1$. Heidi sends $M_2$ to Nelson, who computes $M_3 = M_2 \oplus K_N$. Nelson sends $M_3$ to Heidi, who recovers $K$ as $M_3 \oplus K_H$.

a) Show that $K = M_3 \oplus K_H$.

b) Suppose Eve intercepts $M_1, M_2, M_3$. How can she recover $K$?

2. Bob, Ted, Carol, and Alice want to agree on a common cryptographic key. They publicly choose a large prime $p$ and a primitive root $\alpha$. They privately choose random numbers $b, t, c, a$, respectively. Describe a protocol that allows them to compute $K = \alpha^{btc_a} \pmod{p}$ securely (ignore intruder-in-the-middle attacks).

3. Show how an opponent can use the vulnerability of the following protocol in order to decrypt the messages. Each node $N$ in the network has been assigned a unique secret key $K_n$. This key is used to secure communication between the node and a trusted server. That is, all the keys are stored also on the server. User A, wishing to send a secret message $M$ to user B, initiates the following steps:

**Step1.** A generates a random number $R$ and sends to the server his name $A$, destination $B$, and $E(K_a, R)$.

**Step2.** Server responds by sending $E(K_b, R)$ to $A$.

**Step3.** A sends $E(R, M)$ together with $E(K_b, R)$ to B.

**Step4.** B knows $K_b$, thus decrypts $E(K_b, R)$ to get $R$ and will subsequently use $R$ to decrypt $E(R, M)$ to get $M$.

4. Consider the following protocol for communication between two parties, for example, user A wishing to send message $M$ to user B. In the protocol, $PU_b$ and $PU_a$ are the public keys of B and A, respectively. The symbol $E(PU, M)$ means encryption of the message $M$ with the public key $PU$.

**Step1.** A sends to B the following block: $(A, E(PU_b, [M, A]), B)$.

**Step2.** B acknowledges receipt by sending to A the following block: $(B, E(NU_a, [M, B]), A)$.

Is it possible to simplify the protocol as follows:

**Step1.** A sends B the following block: $(A, E(NU_b, M), B)$.

**Step2.** B acknowledges receipt by sending to A the following block: $(B, E(NU_a, M), A)$.
5. Consider the following protocol, where A and B authenticate each other with the help of a trusted server. A and B have secret keys \( K_{AS} \) and \( K_{BS} \), respectively, with the server.

\[
\begin{align*}
1. & \quad A \rightarrow B: \quad A \\
2. & \quad B \rightarrow A: \quad N_B \\
3. & \quad A \rightarrow B: \quad \{N_B\}^{K_{AS}} \\
4. & \quad B \rightarrow S: \quad \{A, \{N_B\}^{K_{AS}}\}^{K_{BS}} \\
5. & \quad S \rightarrow B: \quad \{N_B\}^{K_{BS}}
\end{align*}
\]

Develop an attack, where an intruder I makes B to accept the run in which I is masquerading as A. In order to achieve this result, the intruder must start two runs with B, in one of which I claims to be A. The two protocol runs continue in parallel but I simply sends a random value \( R \) when asked to respond to the challenge intended for A.

6. Solutions for this exercise must be sent on paper or by email to the lecturer. Deadline as usual on Wednesday 20, at noon.

You can already manipulate expressions containing elliptic curve points. It is enough to know that the set of elliptic curve points is a finite abelian group with \( \infty \) as a neutral element. Consider the following signature scheme:

Let \( E \) be an elliptic curve over \( \mathbb{F}_q \) and let \( N \) be the number of points on the curve. Alice represents a message she wants to sign as a point \( M \in E(\mathbb{F}_q) \). Alice has a secret integer \( a \) and makes public points \( A \) and \( B \), where \( B = aA \).

There is a public function \( f : E(\mathbb{F}_q) \to \mathbb{Z}_N \). Alice performs the following steps:

i) She chooses a random integer \( k \) with \( gcd(k, N) = 1 \).

ii) She computes \( R = M - kA \).

iii) She computes \( s \equiv k^{-1}(1 - f(R)a) \pmod{N} \).

iv) The signed message is \( (M, R, s) \).

Bob verifies the signature as follows:

i) He computes \( V_1 = sR - f(R)B \) and \( V_2 = sM - A \).

ii) He declares the signature valid if \( V_1 = V_2 \).

Show that if Alice performs the required steps correctly, then the verification equation \( V_1 = V_2 \) holds. (This signature scheme is a variant of one due to Nyberg and Ruppel. Both schemes are related to the elliptic curve version of ElGamal signature scheme.)

**Hint:** You should know that if \( N \) is the number of elliptic curve points, then for any point \( P \), \( NP = \infty \). In your calculations, use also \( sk \) without modulus.)