Spring 2023

MATH 1025: Introduction to Cryptography

Homework 5

elliptic eclipse

Problem 1 [5 **pts**] Read Chapter 5.5 in [HPS14]. Write 'Yes' to claim the points.

Use the programs at http://tsvboris.pythonanywhere.com/IntrotoCryptography to solve problems in the following sections.

Elliptic Diffie-Hellman key exchange

Problem 2. Alice and Bob agree to use elliptic Diffie-Hellman key exchange with the prime, elliptic curve, and point

$$p = 2671, E : Y^2 = X^3 + 171X + 853, P = (1980, 431) \in E(\mathbb{F}_{2671}).$$

(a) [10 **pts**] Alice sends Bob the point $Q_A = (2110, 543)$. Bob decides to use the secret multiplier $n_B = 1943$. Which point should Bob send to Alice?

(b) [10 **pts**] What is their secret shared value?

MV-ElGamal cryptosystem

Problem 3**.** We will work with the MV-ElGamal cryptosystem (see page 5 of 'Lectures 21 - 22' notes).

(a) [10 **pts**] Sherlock knows the elliptic curve E and the ciphertext values C_1 and C_2. Show how he can use this knowledge to write down a polynomial equation (modulo p) that relates the two parts of the plaintext message (m_1 and m_2).

(b) [10 **pts**] Alice and Bob exchange a message using MV-ElGamal cryptosystem with elliptic curve $E : Y^2 = X^3 + 7X - 3$ over $\mathbb{F}_{1223}$, with the chosen point $P = (11, 216)$. They use the correspondence $A \leftrightarrow 1, B \leftrightarrow 2, \ldots, Z \leftrightarrow 26$ to transform their text message into a plaintext $m \in \mathbb{F}_{1223}$. Sherlock intercepts the message $(Q_B, C_1, C_2) = ((1086, 292), 37, 681)$ that Bob sent to Alice. Moreover, Watson has found out and told Sherlock that the first part of the plaintext is $m_1 \equiv 89 \leftrightarrow$ HI. Use your answer to part (a) to recover the second part m_2 of the plaintext and the whole message $m = m_1 \| m_2$.

Lenstra's elliptic curve factorization algorithm

Problem 4 [10 **pts**] Use Lenstra's factorization algorithm to factor the number $N = 589$ with the help of elliptic curve $E : Y^2 = X^3 + 4X + 9$ and point $P = (2, 5)$.[1]

[1] **Hint:** prior to every addition of points $Q = kP$ and $Z = sP$ in the group $G(E)$, check if the slope m of the line through these points has denominator (given by $x_Q - x_Z$ if $Q \neq Z$ or $2y_Q$ if $Q = Z$) coprime to N.

Elliptic Curve Digital Signature Algorithm (ECDSA)

Problem 5 [10 **pts**] The *Elliptic Curve Digital Signature Algorithm* (ECDSA) is presented below (Alice signs a document and Bob verifies the signature):

Step 1. **Public Parameter Creation**

A trusted party chooses a finite field $\mathbb{F}_p$, an elliptic curve $E/\mathbb{F}_p$, and a point $P \in E(\mathbb{F}_p)$ of large prime order q, i.e. $qP = \mathcal{O}$, where $\mathcal{O}$ is the unit element.

Step 2. **Key Creation**

Samantha chooses a secret signing key $1 < n_S < q-1$, computes $V = n_S P \in E(\mathbb{F}_p)$ and publishes the verification key V.

Step 3. **Signing**

Samantha chooses a document, i.e. a number $D \pmod q$ and an ephemeral key $e \pmod q$. Then she computes $eP \in E(\mathbb{F}_p)$, followed by

$s_1 \equiv x(eP) \pmod q$ and

$s_2 \equiv (D + n_S s_1)e^{-1} \pmod q$.

Samantha publishes the signature (s_1, s_2).

Step 4. **Verification**

Victor finds $v_1 \equiv Ds_2^{-1} \pmod q$ and $v_2 \equiv s_1 s_2^{-1} \pmod q$. He computes $v_1 P + v_2 V \in E(\mathbb{F}_p)$ and verifies that $x(v_1 P + v_2 V) \equiv s_1 \pmod q$.

Prove that ECDSA works, i.e., check that the verification step succeeds in verifying a valid signature.[2]

[2] **Hint:** you need to check that $x(v_1 P + v_2 V) \equiv s_1 \pmod q$, which is straightforward: $x(v_1 P + v_2 V) \equiv x(Ds_2^{-1} P + s_1 s_2^{-1} n_S P) \equiv \ldots$

Problem 6**.** This problem asks you to compute some numerical instances of ECDSA described above for the public parameters $E : Y^2 = X^3 + 231X + 473, p = 17389, q = 1321, P = (11259, 11278) \in E(\mathbb{F}_p)$. You should begin by verifying that P is a point of order q in $E(\mathbb{F}_p)$.

(a) [10 **pts**] Samantha's private signing key is $s = 542$. What is her public verification key V? What is her digital signature (s_1, s_2) on the document $d = 644$ using the ephemeral key $e = 847$?

(b) [10 **pts**] Tabitha's public verification key is $V = (11017, 14637)$. Is $(s_1, s_2) = (907, 296)$ a valid signature on the document $d = 993$?[3]

Problem 7**.** On the 27th Chaos Communication Congress in 2010, a hacker group called fail0verflow showed that Sony was reusing the same nonce (ephemeral key) for every digitally signed game on Playstation 3. The members could then calculate the private key and create valid signatures for arbitrary files including pirated games.

Suppose that Alice signed two different documents (D_1 and D_2) using the same ephemeral key e.

(a) [10 **pts**] Let D_1 and D_2 be the (hashes) of the signed documents, (s_1, s_2) and $(\widetilde{s}_1, \widetilde{s}_2)$ Alice's signatures. Express the ephemeral key e in terms of the given data.[4]

(b) [5 **pts**] Using your answer in (a), find Alice's private key n_A.

References

[HPS14] J. Hoffstein, J. Pipher, and J. H. Silverman, *An introduction to mathematical cryptography*, 2nd ed., Undergraduate Texts in Mathematics, Springer, New York, 2014.

[3] **Hint:** see Step 4.

[4] **Hint:** as the ephemeral key is the same, $\widetilde{s}_1 = s_1 = x(eP)$.