Introduction to Cryptography

TEK 4500 (Fall 2020)
Problem Set 9

Problem 1.

Read Chapter 9 (Section 9.4 can be skipped) and Chapter 10.1–10.2 in [BR] and Chapter 8 (Section 8.5 can be skipped) and Chapter 9 in [PP].

Problem 2.

a) In a programming language of your choice implement the Square-and-Multiply algorithm for exponentiations in the group $(\mathbf{Z}_p^*, \cdot)$.

b) Let $p = 71232428745345734957989901001 59$. Convince yourself that p is prime.

Hint: Use your implementation from a) to run the Fermat primality test (Lecture 9, slide 26) for some different values $a \in \{2, 3, \ldots, p-1\}$.

c) Suppose Alice and Bob run the Diffie-Hellman protocol using the group $(\mathbf{Z}_p^*, \cdot)$, where p is the prime above. They use 2 as the generator for $(\mathbf{Z}_p^*, \cdot)$. Let Alice's secret value be $a = 2081934828612837167732093031150$, and let $b = 8977101693504993214436898697 14$ be the secret value of Bob. Compute their shared Diffie-Hellman secret.

Computing with elliptic curves

The remaining exercises gives some introduction to computing with elliptic curves. Let $p \geq 5$ be a prime number and let

$$E : y^2 = x^3 + ax + b \pmod{p} \tag{1}$$

be an elliptic curve where $a, b \in \mathbf{F}_p$[1] satisfy $4a^3 + 27b^2 \neq 0 \pmod{p}$[2]. As explained in class, the collection $E(\mathbf{F}_p)$ of all the points $P = (x, y)$ that satisfy (1), together with a

[1]Recall that $\mathbf{F}_p$ just denotes the *combination* of the additive group $(\mathbf{Z}_p, +)$ and the multiplicative group $(\mathbf{Z}_p^*, \cdot)$. That is, we allow ourselves both the option to *add* elements from $\{0, 1, \ldots, p-1\}$ modulo p, as well as *multiplying* elements from $\{1, \ldots, p-1\}$ modulo p. This combination is called a *finite field*.

[2]This requirement is just to avoid some complications. You can safely ignore it.

special point $\mathcal{O}$, is actually an abelian group $(E(\mathbf{F}_p), +)$. Here, the addition operation "+" is *not* simply the component-wise addition of two points. That is, for two points $P = (x_1, y_1), Q = (x_2, y_2) \in E(\mathbf{F}_p)$, it is *not* the case that $P + Q = (x_1 + x_2, y_1 + y_2)$ where both coordinates are taken modulo p. Instead, $P + Q$ is motived by the geometric "chord-and-tangent" procedure defined for an elliptic curve over the real numbers $\mathbf{R}$ (ref. Lecture 8 and 9). Now, for a finite field $\mathbf{F}_p$, the curve defined by (1) does not give a nice graph like in $\mathbf{R}$. However, the algebraic equations that define the chord-and-tangent procedure in $\mathbf{R}$ carry over to $\mathbf{F}_p$.

These equations are not unique and there are many different, equivalent, ways of formulating them. One common way of expressing the addition operation in $(E(\mathbf{F}_p), +)$ is as a number of cases, each dealing with whether the coordinates of P and Q are equal or not (or the identity). Specifically, the following set of equations specify how to add two points $P = (x_1, y_1), Q = (x_2, y_2) \in E(\mathbf{F}_p)$.

E.1) If $Q = \mathcal{O}$ then $P + Q = P$ // by definition, the identity doesn't change the other point

E.2) If $P = \mathcal{O}$ then $P + Q = Q$ // same as above

E.3) If $x_1 = x_2$ and $y_1 = -y_2$ then $P + Q = \mathcal{O}$ // P and Q lie on opposite sides of the x-axis hence are inverses (ref slide 40, Lecture 8)

E.4) If $P = Q$ and $y_1 = 0$ then $P + P = \mathcal{O}$ // special case of slide 40, Lecture 8

E.5) If $P = Q$ and $y_1 \neq 0$ then $P + P = (x_3, y_3)$ where // "point-doubling", slide 41, Lecture 8

$$x_3 = (m^2 - 2x_1) \pmod p \qquad y_3 = (m \cdot (x_1 - x_3) - y_1) \pmod p$$

and

$$m = \frac{3x_1^2 + a}{2y_1} \pmod p$$

E.6) If $P \neq Q$ and $x_1 \neq x_2$ then $P + Q = (x_3, y_3)$ where // "general case", slides 35–39, Lecture 8

$$x_3 = (m^2 - x_1 - x_2) \pmod p \qquad y_3 = (m \cdot (x_1 - x_3) - y_1) \pmod p$$

and

$$m = \frac{y_2 - y_1}{x_2 - x_1} \pmod p$$

For all the remaining problems, elliptic curve addition refer to the equations defined above.

When using E.5) and E.6) you need to be able to compute inverses modulo p when calculating m. In class I mentioned that the common way of doing this is using the Extended

$\mathbf{Exp}^{\mathsf{dlog}}_{G,g}(\mathcal{A})$:

1: $x \stackrel{\$}{\leftarrow} \{0, 1, \ldots, |G| - 1\}$
2: $X \leftarrow g^x$
3: $x' \leftarrow A(X)$
4: **return** $x' \stackrel{?}{=} x$

$\mathbf{Exp}^{\mathsf{dh}}_{G,g}(\mathcal{A})$:

1: $x, y \stackrel{\$}{\leftarrow} \{0, 1, \ldots, |G| - 1\}$
2: $X \leftarrow g^x$
3: $Y \leftarrow g^y$
4: $z \leftarrow A(X, Y)$
5: **return** $g^z \stackrel{?}{=} g^{xy}$

$\mathbf{Adv}^{\mathsf{dlog}}_{G,g}(\mathcal{A}) = \Pr[\mathbf{Exp}^{\mathsf{dlog}}_{G,g}(\mathcal{A}) \Rightarrow \mathsf{true}]$

$\mathbf{Adv}^{\mathsf{dh}}_{G,g}(\mathcal{A}) = \Pr[\mathbf{Exp}^{\mathsf{dh}}_{G,g}(\mathcal{A}) \Rightarrow \mathsf{true}]$

Figure 1: Formal security experiments for the discrete logarithm (DLOG) problem and the Diffie-Hellman problem in a cyclic group $G = \langle g \rangle$.

Euclidean algorithm (EEA). However, there is a neat trick that avoids the need to use the EEA in order to calculate inverses. The trick uses Fermat's Theorem, which recall says that: for any $a \neq 0 \pmod p$ we have

$$a^{p-1} = 1 \pmod p.$$

However, note that we can also write this as

$$a^{p-2} \cdot a = 1 \pmod p$$

In other words: the inverse of a is simply $a^{p-2} \pmod p$!

Problem 3.

Specialize the DLOG experiment $\mathbf{Exp}^{\mathsf{dlog}}_{G,g}(\mathcal{A})$ in Fig. 1 to the case of $G = (E(\mathbf{F}_p), +)$. That is, define which set x is drawn from at Line 1 and how X is created at Line 2 for the specific case of $G = (E(\mathbf{F}_p), +)$. Suppose the generator is P. Do the same with the DH experiment $\mathbf{Exp}^{\mathsf{dh}}_{G,g}(\mathcal{A})$.

Problem 4.

Let E be the elliptic curve $y^2 = x^3 + 3x + 7$ defined over the finite field $\mathbf{F}_{11}$.

a) Show that $P = (8, 9)$ is a point on the curve E.

b) What is the inverse of P? That is, what are the coordinates of $-P$ in the group $(E(\mathbf{F}_{11}), +)$?

$\underline{\mathbf{Exp}^{\mathsf{dlog}}_{(E(\mathbf{F}_p),+),P}(\mathcal{A})}$:

$x \xleftarrow{\$} \{0, 1, \ldots, |E(\mathbf{F}_p)| - 1\}$
$Q \leftarrow xP$
$x' \leftarrow A(Q)$
return $x' \stackrel{?}{=} x$

$\underline{\mathbf{Exp}^{\mathsf{dh}}_{(E(\mathbf{F}_p),+),P}(\mathcal{A})}$:

$x, y \xleftarrow{\$} \{0, 1, \ldots, |E(\mathbf{F}_p)| - 1\}$
$X \leftarrow xP$
$Y \leftarrow yP$
$z \leftarrow A(X, Y)$
return $zP \stackrel{?}{=} xyP$

$$\mathbf{Adv}^{\mathsf{dlog}}_{(E(\mathbf{F}_p),+),P}(\mathcal{A}) = \Pr[\mathbf{Exp}^{\mathsf{dlog}}_{(E(\mathbf{F}_p),+),P}(\mathcal{A}) \Rightarrow \mathsf{true}]$$
$$\mathbf{Adv}^{\mathsf{dh}}_{(E(\mathbf{F}_p),+),P}(\mathcal{A}) = \Pr[\mathbf{Exp}^{\mathsf{dh}}_{(E(\mathbf{F}_p),+),P}(\mathcal{A}) \Rightarrow \mathsf{true}]$$

Figure 2: Formal security experiments for the discrete logarithm (DLOG) problem and the Diffie-Hellman problem specialized to an elliptic curve group $(E(\mathbf{F}_p), +)$ with generator P.

c) Compute $2P = P + P$.

Hint: this is case E.5).

d) Compute $3P = P + P + P = 2P + P$.

e) Compute $4P$.

f) Compute $Q = 5P$.

g) Compute $2Q$.

h) Based on f) and g) what's the order of the cyclic subgroup $\langle P \rangle < (E(\mathbf{F}_{11}), +)$? What's the order of the cyclic subgroup $\langle Q \rangle < (E(\mathbf{F}_{11}), +)$?

Problem 5.

Let E be the elliptic curve $y^2 = x^3 + 5x - 1$ defined over the finite field $\mathbf{F}_{23}$. It turns out that $(E(\mathbf{F}_{23}), +)$ has order 17, i.e., it has 17 elements. Since 17 is a prime number we know that any point $P \neq \mathcal{O}$ is a generator for $(E(\mathbf{F}_{23}), +)$.

a) Show that $P = (3, 8)$ is a point on E.

b) Show that $17P = \mathcal{O}$.

Hint: Compute $2P \mapsto 4P \mapsto 8P \mapsto 16P \mapsto 17P$

References

[BR] Mihir Bellare and Phillip Rogaway. *Introduction to Modern Cryptography*. https://web.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf.

[PP] Christof Paar and Jan Pelzl. *Understanding Cryptography - A Textbook for Students and Practitioners*. Springer, 2010.