CS 259C/Math 250: Elliptic Curves in Cryptography
Homework #2

Due October 26, 2011

Solutions must be handed in in class, handed to Mark (494 Gates), or emailed to Mark (zhandry at cs.stanford.edu) by 4pm on the due date. Your solution to problem 8 must be saved as a SAGE worksheet and emailed to Mark.

Use of SAGE is allowed on any problem. If you use SAGE you must show your work by attaching your computations to the solutions you turn in. Use of LaTeX is encouraged but not required.

Elliptic curves over finite fields

1. (10 points) **Quadratic twists.** Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve over a field K with $\operatorname{char} K \neq 2, 3$. For $d \in K^\times$, the *quadratic twist of* E *by* d is the curve $E^{(d)} : y^2 = x^3 + Ad^2x + Bd^3$.

   (a) Show that $E^{(d)}$ can be transformed over K to the form $dy_1^2 = x_1^3 + Ax_1 + B$.

   Now let $K = \mathbb{F}_q$ be a finite field with $2, 3 \nmid q$, fix a non-square $D \in \mathbb{F}_q^\times$, and let $E' = E^{(D)}$.

   (b) Show that for any $d \in \mathbb{F}_q^\times$, the quadratic twist of E by d is isomorphic over $\mathbb{F}_q$ to either E or E'. We can thus call E' *the* quadratic twist of E.

   (c) Suppose that $\#E(\mathbb{F}_q) = q + 1 - t$. Show that $\#E'(\mathbb{F}_q) = q + 1 + t$. (*Hint:* Use part (1a) and Theorem 4.14 of Washington.)

   (d) Show that $\#E(\mathbb{F}_{q^2}) = \#E(\mathbb{F}_q) \cdot \#E'(\mathbb{F}_q)$.

   (e) Give a counterexample to show that it is not true in general that $E(\mathbb{F}_{q^2}) \cong E(\mathbb{F}_q) \times E'(\mathbb{F}_q)$ as abelian groups.

2. (4 points) **Counting points.** Suppose $p \equiv 3 \pmod 4$, and let $E/\mathbb{F}_p$ be given by $y^2 = x^3 + Ax$. Use the previous exercise and the fact that -1 is not a square in $\mathbb{F}_p$ to show that $\#E(\mathbb{F}_p) = p + 1$, and therefore E is supersingular. (*Hint:* For a given $x \neq 0$, exactly one of $x^3 + Ax$ and $-x^3 - Ax$ is a square in $\mathbb{F}_p$. Use this to deduce that $\#E(\mathbb{F}_p) = \#E^{(-1)}(\mathbb{F}_p)$.)

3. (10 points) **Supersingular curves.** Let E be a supersingular elliptic curve defined over $\mathbb{F}_p$ with $p \geq 5$ prime. Let ϕ be the p-Frobenius endomorphism on E.

   (a) Show that $\phi^2 + p = 0$ as endomorphisms.

   (b) Show that ϕ^2 acts as the identity on $E[p + 1]$, and therefore that $E[p + 1] \subset E(\mathbb{F}_{p^2})$.

   (c) Show that $\#E(\mathbb{F}_{p^2}) = p^2 + 2p + 1$.

(d) Show that $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}_{p+1} \times \mathbb{Z}_{p+1}$.

It follows from Washington Corollary 3.11 that for any $n \geq 2$ not divisible by p, if $E[n] \subset E(\mathbb{F}_p)$ then n divides $p-1$. Use this fact to show the following:

(e) If $p \equiv 1 \pmod 4$, then $E(\mathbb{F}_p)$ is cyclic. If $p \equiv 3 \pmod 4$, then $E(\mathbb{F}_p)$ is either cyclic or isomorphic to $\mathbb{Z}_{(p+1)/2} \times \mathbb{Z}_2$.

By the results of problem 1, we have found a case where $E(\mathbb{F}_{p^2}) \cong E(\mathbb{F}_p) \times E'(\mathbb{F}_p)$.

4. (8 points) **Complex multiplication.** Let E be an elliptic curve given by $y^2 = x^3 + Ax$ over $\mathbb{F}_p$, with $p \geq 3$ prime. Let i be a square root of -1 (in either $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$) and let α be the automorphism of E given by $\alpha(x, y) = (-x, iy)$.

   (a) Compute $\deg(1 + \alpha)$.

   (b) What is the kernel of $1 + \alpha$?

   (c) For integers a, b, let $\phi_{a,b}$ be the endomorphism $[a] + [b]\alpha$. Use Washington Proposition 3.16 to show that $\deg(\phi_{a,b}) = a^2 + b^2$ for all $a, b \in \mathbb{Z}$.

   (d) Show that for any $a, b \in \mathbb{Z}$, there is an endomorphism $\psi_{a,b}$ such that for all $P \in E(\overline{\mathbb{F}}_p)$ we have
$$\psi_{a,b}(\phi_{a,b}(P)) = \phi_{a,b}(\psi_{a,b}(P)) = [a^2 + b^2]P.$$
   The endomorphism $\psi_{a,b}$ is the *dual* of $\phi_{a,b}$.

   If $p \equiv 1 \pmod 4$, then every endomorphism of E is of the form $[a] + [b]\alpha$ for some $a, b \in \mathbb{Z}$. We define addition of endomorphisms by setting $(\beta_1 + \beta_2)(P) = \beta_1(P) + \beta_2(P)$ and we define multiplication of endomorphisms by setting $(\beta_1\beta_2)(P) = \beta_1(\beta_2(P))$. With this structure $\mathrm{End}(E)$ is a ring. Since $\alpha^2 = [-1]$, for the curve in question we have a ring isomorphism
$$\mathrm{End}(E) \cong \mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}; i^2 = -1\}.$$

   We say that E has *complex multiplication by* $\mathbb{Z}[i]$. The dual endomorphism corresponds to the ring element obtained via complex conjugation. The degree function corresponds to the norm map from $\mathbb{Z}[i]$ to $\mathbb{Z}$ given by $z \mapsto |z|^2$.

5. (5 points) **The action of an endomorphism.** Let $p = 677$ and $E/\mathbb{F}_p$ be given by $y^2 = x^3 + x$. The SAGE command `E.abelian_group()` shows that $E(\mathbb{F}_p) \cong \mathbb{Z}_{26} \times \mathbb{Z}_{26}$.

   (a) Give a basis for $E[13]$.

   (b) Give the matrix α_{13} for the action of the endomorphism α (from the previous exercise) with respect to your basis of $E[13]$.

   (c) Show that $(\alpha_{13})^2 = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ as matrices over $\mathbb{F}_{13}$.

   (d) (Bonus, 2 points.) Compute eigenvectors for the action of α on $E[13]$. Specifically, give points $T_1, T_2 \in E[13]$ such that $\alpha(T_i) = [\lambda_i]T_i$ where λ_i are the two square roots of -1 in $\mathbb{F}_{13}$.

Elliptic curve cryptography

6. (12 points) **Definitions of semantic security.** Let $\mathcal{E} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be an encryption scheme. In class we defined semantic security as follows. Let $\mathcal{A}$ be an adversary that plays the following game with a challenger:

   - The challenger computes $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}()$ and sends pk to the adversary.
   - The adversary computes messages m_0, m_1 of the same length and sends them to the challenger.
   - The challenger chooses a bit $b \in \{0, 1\}$, computes $c \leftarrow \mathsf{Enc}(\mathsf{pk}, m_b)$, and sends c to the adversary.
   - The adversary outputs a bit $b' \in \{0, 1\}$.

   We define the *semantic security advantage* of $\mathcal{A}$ to be

   $$\text{SS-Adv}(\mathcal{A}, \mathcal{E}) = \big|\Pr[\mathcal{A}(\mathsf{pk}, c) = 1 : c = \mathsf{Enc}_{\mathsf{pk}}(m_0)] - \Pr[\mathcal{A}(\mathsf{pk}, c) = 1 : c = \mathsf{Enc}_{\mathsf{pk}}(m_1)]\big|.$$

   We say that $\mathcal{E}$ is ϵ*-semantically secure* if for all efficient adversaries $\mathcal{A}$, $\text{SS-Adv}(\mathcal{A}, \mathcal{E}) < \epsilon$.

   Suppose that the message space $\mathcal{M}$ contains a distinguished element '0'. Consider the following modification of the security game:

   - The challenger computes $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}()$ and sends pk to the adversary.
   - The adversary computes $m \in \mathcal{M}$ and sends it to the challenger.
   - The challenger chooses a bit $b \in \{0, 1\}$. If $b = 0$ the challenger computes $c \leftarrow \mathsf{Enc}(\mathsf{pk}, 0)$, while if $b = 1$ the challenger computes $c \leftarrow \mathsf{Enc}(\mathsf{pk}, m)$. The challenger then sends c to the adversary.
   - The adversary outputs a bit $b' \in \{0, 1\}$.

   We define the *real-or-zero advantage* of $\mathcal{A}$ to be

   $$\text{RZ-Adv}(\mathcal{A}, \mathcal{E}) = \big|\Pr[\mathcal{A}'(\mathsf{pk}, c) = 1 : c = \mathsf{Enc}_{\mathsf{pk}}(0)] - \Pr[\mathcal{A}'(\mathsf{pk}, c) = 1 : c = \mathsf{Enc}_{\mathsf{pk}}(m)]\big|.$$

   We say that $\mathcal{E}$ is ϵ'*-RZ-secure* if for all efficient adversaries $\mathcal{A}'$, $\text{RZ-Adv}(\mathcal{A}', \mathcal{E}) < \epsilon'$.

   We will now show that RZ-security is equivalent to semantic security, up to a small constant factor.

   (a) Show that if there is an adversary $\mathcal{A}$ that plays the semantic security game such that $\text{SS-Adv}(\mathcal{A}, \mathcal{E}) \geq \epsilon$, then there is an adversary $\mathcal{A}'$ that plays the RZ-security game such that $\text{RZ-Adv}(\mathcal{A}', \mathcal{E}) \geq \epsilon/2$.

   (b) Show that if there is an adversary $\mathcal{A}'$ that plays the RZ-security game such that $\text{RZ-Adv}(\mathcal{A}', \mathcal{E}) \geq \epsilon$, then there is an adversary $\mathcal{A}$ that plays the semantic security game such that $\text{SS-Adv}(\mathcal{A}, \mathcal{E}) \geq \epsilon$.

   Now suppose that the ciphertext space $\mathcal{C}$ always admits an efficient sampling algorithm. Consider the following modification of the security game:

   - The challenger computes $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}()$ and sends pk to the adversary.

- The adversary computes $m \in \mathcal{M}$ and sends it to the challenger.
- The challenger chooses a bit $b \in \{0,1\}$. If $b = 0$ the challenger samples $c \leftarrow \mathsf{Enc}(\mathsf{pk}, m)$, while if $b = 1$ the challenger computes $c \overset{\text{R}}{\leftarrow} \mathcal{C}$.[1] The challenger then sends c to the adversary.
- The adversary outputs a bit $b' \in \{0,1\}$.

We define the *real-or-random ciphertext advantage* of $\mathcal{A}$ to be

$$\text{RRC-Adv}(\mathcal{A}, \mathcal{E}) = \left| \Pr[\mathcal{A}(\mathsf{pk}, c) = 1 : c = \mathsf{Enc}_{\mathsf{pk}}(m)] - \Pr[\mathcal{A}(\mathsf{pk}, c) = 1 : c \overset{\text{R}}{\leftarrow} \mathcal{C}] \right|.$$

We say that $\mathcal{E}$ is *ϵ-RRC-secure* if for all efficient adversaries $\mathcal{A}$, $\text{RRC-Adv}(\mathcal{A}, \mathcal{E}) < \epsilon$.

We will now show that RRC-security is not equivalent to semantic security. Let $\mathcal{E} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be an ϵ-semantically secure encryption scheme. Suppose Enc outputs ciphertexts in $\{0,1\}^n$. Define an encryption scheme $\mathcal{E}' = (\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ as follows:

- Gen' runs Gen and outputs pk, sk.
- Enc' on input m computes $c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m)$ and outputs $c' = c \| 0 \in \{0,1\}^{n+1}$ (i.e., c concatenated with a zero bit).
- Dec' on input $c' = c|b$ with $c \in \{0,1\}^n$ and $b \in \{0,1\}$ outputs $\mathsf{Dec}_{\mathsf{sk}}(c)$.

(c) Show that $\mathcal{E}'$ is ϵ-semantically secure. Specifically, show that if there is an adversary $\mathcal{A}$ such that $\text{SS-Adv}(\mathcal{A}, \mathcal{E}') \geq \epsilon$, then there is an adversary $\mathcal{B}$ such that $\text{SS-Adv}(\mathcal{B}, \mathcal{E}) \geq \epsilon$.

(d) Show that $\mathcal{E}'$ is not not ϵ-RRC-secure for any $\epsilon \leq 1/2$. Specifically, give an algorithm $\mathcal{A}$ such that $\text{RRC-Adv}(\mathcal{A}, \mathcal{E}') = 1/2$.

7. (4 points) **Decision Diffie-Hellman.** Let $\mathbb{G}$ be an abelian group of order $2r$ where r is prime, and let g be a generator of $\mathbb{G}$ (i.e., an element of order $2r$). Show that the DDH problem is not hard in $\mathbb{G}$, by exhibiting an algorithm $\mathcal{A}$ that can distinguish $\{g, g^a, g^b, g^{ab}\}$ from $\{g, g^a, g^b, g^c\}$ with advantage $1/2$ for random $a, b, c \in [0, 2p-1]$.

   Specifically, define your algorithm $\mathcal{A}$ to take as input four elements of $\mathbb{G}$ and output 0 or 1, and show that when a, b, c are uniformly random in $[0, 2p-1]$, we have

$$\left| \Pr[\mathcal{A}(g, g^a, g^b, g^{ab}) = 1] - \Pr[\mathcal{A}(g, g^a, g^b, g^c) = 1] \right| = \frac{1}{2}.$$

   (More generally, the DDH problem in $\mathbb{G}$ is only as hard as the problem in the *smallest* prime-order subgroup of $\mathbb{G}$. In contrast, the discrete log problem in $\mathbb{G}$ is as hard as the problem in the *largest* prime-order subgroup of $\mathbb{G}$. Thus the assumption that DDH is infeasible in $\mathbb{G}$ appears to be significantly stronger than the assumption that discrete log is infeasible in $\mathbb{G}$.)

8. (10 points) **ElGamal encryption.** The goal of this exercise is to encrypt your name using the ElGamal cryptosystem. Let $p = 2^{192} - 2^{64} - 1$. Let E be the elliptic curve over $\mathbb{F}_p$ given by

$$E : y^2 = x^3 - 3x + 2455155546008943817740293915197451784769108058161191238065.$$

[1] The notation $x \overset{\text{R}}{\leftarrow} X$ means that the variable x is chosen to be a uniformly random element of the set X.

Let (P, Q) be an ElGamal public key given by

$$\begin{aligned} P &= (60204628237568865675821348058752611191669897663688468481 8, \\ &\quad 17405033229362203140485755228021941036402348892738665064 1) \\ Q = [a]P &= (36639631139692915444699262805386122983673835142020289869 22, \\ &\quad 10421310403784908333789056122286665529574048250048158843 20) \end{aligned}$$

The SAGE worksheet "Homework2" (available on the course website) has E, P, and Q already entered. The worksheet also has functions `str_to_int` and `int_to_str` that use base 36 notation to convert (alphanumeric, case-insensitive) strings of length n to integers in $[0, 36^n)$, and vice versa.

(a) Write a function `int_to_point(n,E)` that takes an integer $n \in [0, 36^{25}]$ and returns a point on the curve E.

(b) Write a function `point_to_int(P)` that takes a point P on E and returns an integer, such that for n in $[0, 36^{25}]$ we have

$$\texttt{point\_to\_int}(\texttt{int\_to\_point}(\texttt{n}, \texttt{E})) = n.$$

Use the function `test_inverses` in the worksheet to verify your work.

(c) Write a function `encrypt(P,Q,s)` that computes the encryption of the string s using the ElGamal public key (P, Q). Make sure your function does not leak the randomness used in the encryption!

(d) Compute an encryption of your name using your `encrypt` function. (If your name is longer than 25 characters, use the first 25 characters only.)

(e) (Bonus, 2 points.) How did I choose the curve E and the point P? (*Hint:* Google knows the answer.)

9. (4 pionts) **Consequences of bad randomness.** Suppose the random values k used by the signer in the Schnorr signature scheme are generated using the linear congruential generator $k_{i+1} = Ak_i + B \pmod{r}$ for some $1 \leq A, B < r$ (recall r is the order of the group in which computations are done). Suppose an adversary knows A and B and sees two messages m and m' and signatures (R, s) and (R', s') on m and m', respectively, that were generated using consecutive outputs k_i and k_{i+1} of the generator. Show how the adversary can determine (with high probability) the secret key a.