1. (8 points) **Multi-user encryption.** In this problem we will convert Joux’s three-way key exchange protocol into a “multi-user” encryption scheme. 

Let $E/F_p$ be a supersingular elliptic curve with $P \in E(F_p)$ a point of (prime) order $n$. Let $G = \langle P \rangle$ and define the modified Weil pairing $\hat{e}: G \times G \to \mu_n \subset F_p^\times$ as in class. (In particular, $\hat{e}(P,P)$ is a generator of $\mu_n$.) We assume that $pp = (E, \hat{e}, P)$ are public parameters known to everyone in the system.

Suppose Alice and Bob execute their parts of the three-way key exchange protocol. Specifically, Alice chooses $a \overset{R}{\leftarrow} [1, n]$ and publishes $Q_A = [a]P$, while Bob chooses $b \overset{R}{\leftarrow} [1, n]$ and publishes $Q_B = [b]P$.

(a) Show how a third party can encrypt a message $M \in \mu_n$ to Alice and Bob simultaneously. Specifically, give an encryption algorithm $\text{Enc}(pp, Q_A, Q_B, M)$ and a decryption algorithm $\text{Dec}(pp, sk, C)$ that satisfy the following correctness property

$$\text{Dec}(pp, a, \text{Enc}(pp, Q_A, Q_B, M)) = \text{Dec}(pp, b, \text{Enc}(pp, Q_A, Q_B, M)) = M.$$ 

*Hint: Construct a variant of Boneh-Franklin IBE that doesn’t use any hash functions.*

(b) Prove that if the BDDH assumption holds for $G$, then the system in (1a) is semantically secure against any attacker not knowing $a$ or $b$. Specifically, suppose you are given a BDDH challenge $P, aP, bP, cP, \gamma$ and an adversary $A$ that can distinguish the encryption of a chosen message $M$ from the encryption of a random message $M'$. Design an algorithm $B$ that uses $A$ as a subroutine and decides whether $\gamma = \hat{e}(P,P)^{abc}$.

If we had a more powerful map, we could extend this functionality to more than two receivers. Specifically, suppose that we had a nondegenerate, symmetric, $\ell$-linear map $\bar{e}: G^\ell \to \mu_n$. In particular, $\bar{e}$ satisfies

$$\bar{e}([c_1]P, \ldots, [c_\ell]P) = \bar{e}(P, \ldots, P)^{c_1 \cdots c_\ell}.$$
(c) Suppose that $\ell$ parties each choose some $a_i \overset{R}{\leftarrow} [1, n]$ and publish $Q_i = [a_i]P$. Let $M \in \mu_n$ be a message. Generalize your system from above: give $\text{Enc}$ and $\text{Dec}$ algorithms such that any party can use her secret key and the public information to decrypt the ciphertext. (You do not need to give a security proof.)

(d) (Bonus, 2 points.) Modify the $\ell$-party system to allow encrypting to subsets of users. Specifically, describe a modified set of public parameters and give an $\text{Enc}$ algorithm that takes the public information, a subset $S \subset \{1, \ldots, \ell\}$, and a message $M$, and outputs a ciphertext $C$. Give a $\text{Dec}$ algorithm that takes the public information and a user’s secret key $a_i$ and outputs a message. The correctness condition is that for any $S \subset \{1, \ldots, \ell\}$, if $i \in S$ then

$$\text{Dec}(\text{pp}, a_i, \text{Enc}(\text{pp}, \{Q_i\}, S, M)) = M.$$ 

You do not need to provide a security proof, but you should make sure there is no obvious way for the users outside of $S$ to combine their secret keys to decrypt the message. (Hint: consider adding random points $R_i$ to the public parameters.)

The $\ell$-party construction requires an efficiently computable $\ell$-linear map between groups where the discrete logarithm problem is hard. Unfortunately, the largest $\ell$ for which we know how to construct such a map is $\ell = 2!$.

2. (6 points) Signatures from IBE. Moni Naor observed that any IBE scheme can be converted to a signature scheme: the signature $\sigma$ on a message $m$ is the IBE secret key corresponding to $\text{id} = m$, and to verify a signature we test whether the given key $\sigma$ can decrypt the IBE encryption of a random message.

Specifically, suppose that $\mathcal{E} = (\text{Setup}, \text{Extract}, \text{Enc}, \text{Dec})$ is an IBE scheme. We construct a signature scheme $\mathcal{S}$ as follows:

- $\text{Gen}()$: Run the IBE Setup algorithm to obtain public parameters $\text{pp}$ and a master key $\text{mk}$. Output $\text{pk}_S = \text{pp}$ and $\text{sk}_S = (\text{pp}, \text{mk})$.
- $\text{Sign}(\text{sk}_S, m)$: Interpret $\text{sk}_S$ as an IBE master key $\text{mk}$ and public parameters $\text{pp}$, and interpret the message $m$ as an identity $\text{id}$. Output $\sigma \leftarrow \text{Extract}(\text{pp}, \text{mk}, \text{id})$.
- $\text{Verify}(\text{pk}_S, m, \sigma)$: Interpret $\text{pk}_S$ as IBE public parameters $\text{pp}$, interpret $m$ as an identity $\text{id}$, and interpret $\sigma$ as an IBE secret key $\text{sk}_\text{id}$. Choose a random message $\tilde{m}$ in the IBE message space. Output “accept” if

$$\text{Dec}(\text{pp}, \text{Enc}(\text{pp}, \text{id}, \tilde{m}), \text{sk}_\text{id}) = \tilde{m}.$$ 

Output “reject” otherwise.

Show that if $\mathcal{E}$ is a semantically secure IBE scheme, then $\mathcal{S}$ is a secure signature scheme. Specifically, assume that there is a signature adversary $A$ that outputs a valid forgery for $\mathcal{S}$ with probability $\epsilon$. Construct an IBE adversary $B$ that uses $A$ as a subroutine and breaks $\mathcal{E}$ with advantage $\epsilon - 1/r$, where $r$ is the size of the message space for $\mathcal{E}$. You will need to show:

- how $B$ responds to $A$’s signature queries;
- how $B$ uses $A$’s forgery to distinguish the encryption of a chosen message $M$ from that of a random message $M'$;
that the advantage of $B$ in the IBE security game is $\epsilon - 1/r$.

Note that you don’t need to worry about any hash function or “random oracles” — you just need to work with the definitions of security. You may assume that Dec is a deterministic algorithm that always outputs a message in the IBE message space.

(Bonus, 2 points.) Why must Verify be randomized? Specifically, say where your security proof fails if we use the following Verify' algorithm: output “accept” if and only if

$$\text{Dec}(\text{pp}, \text{Enc}(\text{pp}, \text{id}, 0), \text{sk}_\text{id}) = 0.$$  

3. (8 points) Asymmetric BLS signatures. The asymmetric version of Boneh-Lynn-Shacham signatures uses an elliptic curve $E$, two order-$n$ subgroups $G_1, G_2 \subset E[n]$, and a nondegenerate, efficiently computable, bilinear map $e: G_1 \times G_2 \rightarrow \mu_n$. The proof of security in this setting requires an efficiently computable isomorphism $\psi: G_2 \rightarrow G_1$. When $E$ is supersingular we can take $G_1 = G_2 = E[n] \cap E(F_p)$, $e$ to be the modified Weil pairing $\hat{e}$, and $\psi$ to be the identity map. In this problem we will investigate a candidate for the map $\psi$ on more general curves.

Let $\phi$ be the $p$-Frobenius endomorphism. For a fixed $k \geq 1$, define the trace map $\text{Tr}$ by

$$\text{Tr}(P) = \sum_{i=0}^{k-1} \phi^i(P).$$

(a) Show that $\text{Tr}$ maps points defined over $\mathbb{F}_{p^k}$ to points defined over $\mathbb{F}_p$. Specifically, show that if $P \in E(\mathbb{F}_{p^k})$, then $\text{Tr}(P) \in E(\mathbb{F}_p)$.

Suppose that $E(\mathbb{F}_p)$ has a point of prime order $n$ and $E$ has embedding degree $k \geq 2$ with respect to $n$ (i.e., $E[n] \subset E(\mathbb{F}_{p^k})$). Assume $n \nmid kp$. Recall from Homework 3 that $\phi$ has eigenvalues 1 and $p$ on $E[n]$.

(b) Show that if $P \in E[n]$ is an eigenvalue of $\phi$ with eigenvalue $p$, then $\text{Tr}(P) = \infty$. (Hint: factor $p^k - 1$.)

(c) Show that for any $P \in E[n]$ with $P \neq \infty$, the point $[k]P - \text{Tr}(P)$ is an eigenvector of $\phi$ with eigenvalue $p$.

(d) Let $P$ be a point in $E(\mathbb{F}_p)$ of order $n$, and let $G_1 = \langle P \rangle$. For any $R \in E[n]$, let $G_R = \langle R \rangle$. Show that if $R$ is chosen at random from $E[n]$, then with probability $(1 - 1/n)^2$ it holds that:

- $e_n(P, R)$ is a generator of $\mu_n \subset \mathbb{F}_{q^k}$, and
- $\text{Tr}: G_R \rightarrow G_1$ is an isomorphism.

(Here $e_n$ is the usual Weil pairing.)

4. (10 points) BGN encryption in prime-order groups. In this exercise we show how to achieve the functionality of the Boneh-Goh-Nissim encryption scheme without using composite-order groups. Let $E/\mathbb{F}_p$ be an elliptic curve and $P \in E(\mathbb{F}_p)$ a point of prime order $n$. Define the following algorithms:
5. (6 points) Pairing-friendly curves. For this problem you will want to consult problem #9 of Homework 3.

(a) Find a field $\mathbb{F}_{2^d}$ and a supersingular elliptic curve $E/\mathbb{F}_{2^d}$ of the form $y^2 + y = x^3 + Ax$ (with $A \in \mathbb{F}_{2^d}$) such that

- $E(\mathbb{F}_{2^d})$ has a subgroup of prime order $r > 2^{160}$. 

(b) Give a $\text{Dec}$ algorithm that takes a ciphertext $(A, B)$ and outputs $m$. (Hint: first recover $[m]P$, then do a brute-force discrete log calculation.)

(c) Let $(A_1, B_1)$ and $(A_2, B_2)$ be encryptions of messages $m_1, m_2$ respectively. Give an algorithm $\text{Add}$ that takes the public key $pk$ and the two ciphertexts as input, and outputs a random encryption of $m_1 + m_2$. The output ciphertext should be distributed as if the message $m_1 + m_2$ was encrypted with fresh randomness. Note that $\text{Add}$ does not know either $m_1$ or $m_2$.

(d) Now suppose that $P' \in E(\mathbb{F}_{p^k})$ is a point of order $n$ such that $e_n(P, P') \neq 1$. Let $G_2 = \langle P' \rangle$, and let $pk' = (P', Q', R', S')$ and $sk' = (a', b', c')$ be public and secret keys obtained by running $\text{Setup}()$ using the group $G_2$. Suppose we have

$$\textbf{(A, B)} = \text{Enc}(pk, m) \quad \text{and} \quad \textbf{(C, D)} = \text{Enc}(pk', m').$$

(Here $A, B \in G_1$ and $C, D \in G_2$.) Let $\text{Mult}$ be an algorithm that takes as input the two public keys and the two ciphertexts and outputs the tuple $(w, x, y, z) \in \mu_n^4$, where

$$w = e_n(A, C), \quad x = e_n(A, D), \quad y = e_n(B, C), \quad z = e_n(B, D).$$

Show how to recover $e_n(P, P')^{m-m'}$ from $(w, x, y, z)$ and the two secret keys $sk, sk'$.

We conclude that if the DDH assumption holds in $G_1$ and $G_2$, then we have a semantically secure cryptosystem that encrypts small messages, supports arbitrarily many additions of encrypted messages, and allows one multiplication of encrypted messages — exactly the functionality of the BGN cryptosystem. (Technically we also need to show how to rerandomize the tuple $(w, x, y, z)$, but we ignore this for now.)

It is believed that if $E$ is an ordinary (i.e., non-supersingular) elliptic curve, then the DDH assumption holds in the subgroups $G_1$ and $G_2$ where $G_1$ is the 1-eigenspace of Frobenius (i.e., points of order $n$ in $E(\mathbb{F}_{p^k})$) and $G_2$ is the $p$-eigenspace of Frobenius (i.e., points of order $n$ with trace zero).
• $E$ has embedding degree 4 with respect to $r$.
• The Weil pairing on $E[r]$ takes values in a field of size at least $2^{1000}$.

(*Hint: You should find $d$ and $r$ before starting your search for $E$.*)

(b) Find a field $\mathbb{F}_{3^d}$ and a supersingular elliptic curve $E/\mathbb{F}_{3^d}$ of the form $y^2 = x^3 + Ax + 1$ (with $A \in \mathbb{F}_{3^d}$) such that
• $E(\mathbb{F}_{3^d})$ has a subgroup of prime order $r > 2^{160}$.
• $E$ has embedding degree 6 with respect to $r$.
• The Weil pairing on $E[r]$ takes values in a field of size at least $2^{1000}$.

(c) Define

$$p(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1$$
$$r(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1$$

Find an integer $\alpha > 2^{63}$ such that $p(\alpha)$ and $r(\alpha)$ are both prime. Construct an elliptic curve $E/\mathbb{F}_p(\alpha)$ of the form $y^2 = x^3 + B$ such that $\#E(\mathbb{F}_p(\alpha)) = r(\alpha)$. Show that $E$ has embedding degree 12 with respect to $r(\alpha)$.
This curve is a *Barreto-Naehrig curve* and is the curve of choice for pairing applications at the 128-bit security level.