Problem 1. Let $\Pi = (K, E, D)$ be an IV-based encryption scheme. Consider the following notion of security that we will call indistinguishability from random bits under a chosen-plaintext attack (IND$^\$-CPA). Let $A$ be a nonce-respecting adversary that takes one oracle, has time complexity $t$, asks $q$ queries, these totalling $\mu$ bits in length. Then define the IND$^\$-CPA advantage of $A$ against $\Pi$

\[
\text{Adv}_{\Pi}^{\text{ind$^\$-cpa}}(A) = 2 \cdot \Pr \left[ \text{Exp}_{\Pi}^{\text{ind$^\$-cpa}}(A) = 1 \right] - 1.
\]

Prove the following informal statement: if $\Pi$ is IND$^\$-CPA secure against nonce-respecting adversaries, then $\Pi$ is IND-CPA secure against nonce respecting adversaries. Summarize the result of your proof in a nice theorem statement, please.

Problem 2. Let $\Pi = (K, E, D)$ be an IV-based encryption scheme, with IV-space $\mathcal{V}$, that is a mode-of-operation over an underlying blockcipher $E: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$. On input $N \in \mathcal{V}$ and $M \in (\{0,1\}^n)^+$, $E^N_K(M)$ operates as follows. It parses $M$ into $n$-bit blocks $M_1, \ldots, M_\ell$, sets $C_0 \leftarrow N$, and then for all $i \in \{1,2,\ldots,\ell\}$ it sets $C_i \leftarrow C_{i-1} \oplus E_K(M_i)$. Finally, it returns $C_1 \parallel C_2 \parallel \cdots \parallel C_\ell$ as the ciphertext. (Assume that $E^N_K(M) = \perp$ for all $M \notin (\{0,1\}^n)^+$.)

Decryption occurs in the obvious way.

You are to prove or disprove this claim: if $E$ is a secure PRF, then $\Pi$ is iv-IND-CPA secure. (That is, secure when the IV $N$ is randomly sampled prior to encrypting each message.) To disprove the claim, give a carefully stated, nicely formatted attack on the iv-IND-CPA security of $\Pi$. To prove the claim, give a convincing proof sketch (at least) that $E$ PRF-secure $\Rightarrow \Pi$ iv-IND-CPA secure.

Problem 3. Consider the following instantiation of CTR-mode encryption over a function family $E: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$. Key generation is as normal, $K \leftarrow \{0,1\}^k$. To encrypt, $E^V_K(M)$ is
defined exactly as in CTR-mode, except that the inputs to $E_K$ are not $V \parallel \langle i \rangle$, but rather $\langle V + i \rangle$ where $V$ is converted to an integer prior to addition (which is mod $2^n$ since the input to $E_K$ is only $n$-bits long). So to encrypt message $M = M_1 M_2 \cdots M_b$ (where $|M_i| = n$ for all $i$ except perhaps $i = b$), one returns the ciphertext blocks $C_i \leftarrow M_i \oplus E_K((V + i))$. Decryption works in the obvious way.

First, show that this version of CTR-mode is not IND-CPA against nonce-respecting adversaries. That is, give an adversary that gains advantage close to one in the nonce-IND-CPA game, with small $q, \sigma, t$. For your advantage analysis, assume that $E_K$ is replaced by a random function $\rho$.

Second, come up with a fix! (And no, changing the inputs back to $V \parallel \langle i \rangle$ is not a fix.) Assume that you are stuck with this implementation, i.e. you can only make a library call to a function that on input $(K, V, M)$ returns a ciphertext computed as above. Your job is to wrap some crypto around this, so that the resulting scheme is nonce-IND-CPA. Prove that your new scheme is nonce-IND-CPA. Yes, prove. Figure out what assumptions you need to build upon, do any necessary reductions, work out the advantages, and write a nice, clean theorem statement.

**Problem 4.** Let $F: \{0, 1\}^k \times \{0, 1\}^* \rightarrow \{0, 1\}^n$ be a function family. Fix sets $\mathcal{V}, \mathcal{H}$, and consider the encryption scheme (with associated data) $\Pi = (K, \mathcal{E}, \mathcal{D})$ with the following component algorithms.

- Key generation $\mathcal{K}$ samples $K \leftarrow \{0, 1\}^k$
- Encryption $\mathcal{E}: \mathcal{K} \times \mathcal{V} \times \mathcal{H} \times \{0, 1\}^* \rightarrow \{0, 1\}^*$ is defined to be $\mathcal{E}(K, V, H, M) = E_K^{V, H}(M) = M \parallel F_K(V \parallel H \parallel M)$
- Decryption $\mathcal{D}: \mathcal{K} \times \mathcal{V} \times \mathcal{H} \times \{0, 1\}^* \rightarrow \{0, 1\}^* \cup \{\perp\}$ is defined as follows. On input $(V, H, C)$, (1) parse $X, T \leftarrow C$ where $|T| = n$; (2) if $T = F_K(V \parallel H \parallel X)$, return $X$; otherwise return $\perp$

Prove that $\Pi$ is AUTH-secure under the assumption that $F$ is a secure PRF.

To remind you, the AUTH notion (for AEAD schemes) is defined in Figure 1. To be clear, the adversary’s left oracle $\mathcal{E}_K^{(\cdot)}(\cdot)$ takes input $(V, H, M)$ and returns $\mathcal{E}_K^{V, H}(M)$. The Auth-advantage of $A$ against $\Pi$ by $\text{Adv}_{\Pi}^{\text{auth}}(A) = 2 \cdot \Pr[\text{Exp}_{\Pi}^{\text{auth}}(A) = 1] - 1$. To prevent trivial wins, we forbid Auth-adversaries from asking $(V, H, C)$ to the right oracle if $C$ was previously returned by the left oracle in response to a query of the form $(V, H, M)$. In other words, replay doesn’t count.

**Problem 5.** Let $E: \{0, 1\}^k \times \{0, 1\}^* \rightarrow \{0, 1\}^*$ be a function family with the following properties. For every key $K \in \{0, 1\}^k$, and for any length $\ell > 0$: (1) if $|M| = \ell$ then $|E_K(M)| = \ell$, and (2) $E_K$ is a permutation. That is, $E$ is a variable-input-length (VIL), length-preserving permutation – for every $\ell$, $E_K$ is a permutation over $\{0, 1\}^\ell$.

Now, consider the following way to build an IV-based encryption scheme. Let $v, s > 0$ be fixed parameters and let encryption be defined as $\mathcal{E}_K^N(M) = E_K(N \parallel M \parallel 0^s)$, where $N \in \{0, 1\}^v$. For
decryption, on input \((N, C)\): parse \(E_K^{-1}(C)\) as \(N', M', Z\) where \(|Z| = s\) and \(|N'| = v\); if \(Z = 0^s\) and \(N' = N\) then return \(M'\); otherwise return \(\perp\).

Say we extend the PRP security notion to VIL objects like \(E\). Namely, that for a secret, random key \(K\), it is hard to distinguish between \(E_K(\cdot)\) and \(\Pi(\cdot)\), where \(\Pi\) is a family of random permutations, one for each length \(\ell\). That is, if you ask the oracle an \(\ell\)-bit message \(M\), you either get back \(E_K(M)\), or you get back \(\Pi(M) = \pi_\ell(M)\), where \(\pi_\ell\) is random element of \(\text{Perm}(\ell)\). Let’s call that the VIL-PRP notion. Likewise, we can extend the SPRP notion to VIL objects, i.e. oracles \(E_K(\cdot), E_K^{-1}(\cdot)\) vs. \(\Pi(\cdot), \Pi^{-1}(\cdot)\). Let’s call that the VIL-SPRP notion.

Explain why the encryption scheme defined by \(E, D\) is both IND$-$CPA and AUTH secure under the assumption that \(E\) is a secure VIL-SPRP. No proof required (although you are welcome to give it a go), just think through it and give me a convincing, informal explanation. How do the parameters \(v, s\) figure into security?