Problem 1. (30 points.) Let $N_1, N_2, N_3$ be RSA moduli of length $k$. Give an efficient (in $k$) algorithm that on inputs $X^3 \mod N_i$ for all $i \in \{1, 2, 3\}$ outputs $X$, for any $X < \min\{N_1, N_2, N_3\}$.

Problem 2. (30 points.) Consider a “ naïvely deterministic” variant of the DSA signature scheme in which instead of executing $k \leftarrow \mathbb{Z}_q^*$ in the signing algorithm, this line is executed in the key-generation algorithm and the resulting value of $k$ is included (along with $x$) in the secret key. Then in the signing algorithm the same value of $k$ is used each time. That is, a signature on $m$ is $(r, s)$ where $r \leftarrow g^k \mod p \mod q$ and $s \leftarrow (H(m) + xr) \cdot k^{-1} \mod q$, for secret key $sk = (x, k)$.

Show that this variant of DSA is not UF-CMA secure. Namely, present a practical adversary against it achieving high UF-CMA advantage with low resource usage. Formally analyze the advantage and resource usage of your presented adversary.

Problem 3. (30 points.) Let $\mathcal{K}_{rsa}$ be an RSA generator with modulus length $k$. Consider the digital signature scheme $\mathcal{DS} = (\mathcal{K}, \mathcal{S}, \mathcal{V})$ given below, where $M \in \mathbb{Z}_N^*$:

\begin{align*}
\text{Alg } \mathcal{K}: & \quad (N, p, q, e, d) \leftarrow \mathcal{K}_{rsa} \\
& \quad A, B \leftarrow \mathbb{Z}_N^* \\
& \quad \text{Return } ((N, e), (N, d, A, B)) \\
\text{Alg } \mathcal{S}((N, d, A, B), M): & \quad W \leftarrow AM + B \mod N \\
& \quad Y \leftarrow W^d \mod N \\
& \quad \text{Return } (W, Y) \\
\text{Alg } \mathcal{V}((N, e), (W, Y)): & \quad \text{If } W = Y^e \mod N \text{ then return 1} \\
& \quad \text{Else return 0}
\end{align*}

Show that $\mathcal{DS}$ is not UF-CMA secure. Namely, present a practical adversary against it achieving high UF-CMA advantage with low resource usage. Formally analyze the advantage and resource usage of your presented adversary.

Problem 4. (10 points.) Read a recent popular news article about cryptography and write a short (3 sentence max) critique. Submit a link to the article with your response. Here are the types of questions you can answer: Does the article appear factually correct? Does it do a good job of conveying the issues at hand to the lay public? Is there anything you would add?