Round 1 Crypto

1. HEMTN SSHSR SETET STRIA ELATH MUEET YO
   Substitution, transposition, or shift? **transposition**

2. Why is cipher block chaining (CBC) mode considered preferable to electronic codebook mode (ECB)?
   It prevents repeated patterns in the plaintext from being apparent in the ciphertext

3. Compute $14^3 \mod 3$. **2**

4. Name a problem RSA has when used without OAEP. **Malleability.** An active attacker can replace $E(m)$ with $E(m^k)$, for example.


Round 2 Hashes. Bob has two hash functions, $f$ and $g$. He knows that one of them is collision-resistant (and the other isn’t), but he’s not sure which is which. He wants to create a new hash function $h$ which is definitely collision-resistant. Evaluate each of the following proposals, and either give a proof that it is definitely collision-resistant, or describe a counterexample (as usual, the $\circ$ symbol denotes concatenation):

1. $h(x) = f(x) \circ g(x)$ **YES**

2. $h(x) = f(g(x))$ **NO**

3. $h(x) = f(g(x)) \circ g(f(x))$ **NO**

4. Explain the difference between strong collision resistance and a second pre-image attack? Quantify this difference in how long it would take to brute-force the attack for a perfect hash function of $n$ bits. **Strong collision resistance means it is hard to find any pair of messages that collide. A second preimage attack means finding a collision for a specific message $m$. You would expect a second preimage attack to take $2^{n-1}$ operations on average, whereas just finding a collision would take approximately $2^n$.**

5. Estimate the probability that there are two non-identical files, somewhere on the planet Earth, right now, that have the same MD5 hash code. **Probability is 1. Many collisions have been found for MD5.**

6. Do the same for SHA-1. State your assumptions and cite all references used. **This is harder to say. Assuming someone hasn’t broken SHA-1 in secret, there are many fewer than $2^{80}$ files around, so it is unlikely.**

Round 3 Authentication

1. What is the purpose of the public and private salts in a password file? **To make offline password breaking attacks more difficult (prevent rainbow tables).**

2. To achieve confidentiality and integrity protection, how should you best combine authentication and encryption? **First encrypt, then MAC.**

3. Suppose that an adversary can see all the keys that you type on your keyboard. Is it possible for you to securely type in a password to a program that is running on your machine? You can assume that the adversary can only log your keystrokes, and that you can make small modifications to the program which accepts your password. **Yes, for example you can type the password with a mouse on a keyboard on the screen.**
4. Assuming a very large message, and public user keys, describe what information should be included in Bob sending an encrypted, signed message to Alice and Carol. Bob might first set up a session key with Alice and Carol, then proceed as in the next step, or, hash the message and sign it. So the message includes:

\[ C_A = E_{K_A}(m) \text{ and } S_{K_B}(\text{Hash}(C_A)) \]

\[ C_C = E_{K_C}(m) \text{ and } S_{K_B}(\text{Hash}(C_C)) \]

5. Assuming a very large message, and shared keys between each pair of users, describe what information would be included in Bob sending an encrypted, integrity-protected message to Alice and Carol.

\[ C_{AB} = E_{K_{AB}}(m) \text{ and } \text{HMAC}(C_{AB}, K_{AB}) \]

\[ C_{CB} = E_{K_{CB}}(m) \text{ and } \text{HMAC}(C_{CB}, K_{CB}) \]