# CS 161 Fall 2006 — Computer Security Joseph/Tygar — HW 2 Solutions

**Solutions to exercises:**

1. **(20 pts.) A Cryptographic Protocol**

   It is vulnerable to a man-in-the-middle attack. An attacker could intercept the original message, replace it with their own bit string, and pass the string to your partner. Your partner will XOR the message with the key and send it back. By XORing the response with the original string, the attacker can recover the key, and then can XOR the key with the message you sent and respond with the correct message.

   Alternatively, the attacker could XOR the two messages and directly recover the key.

2. **(20 pts.) RSA Eavesdropping**

   Eve uses the Chinese Remainder Theorem. Let $n_A = p_A q_A$, $n_B = p_B q_B$, and $n_C = p_C q_C$. With high probability, each of the p's and q's will be distinct. Consider modulus $n_X = p_A p_B p_C q_A q_B q_C$. Since $n_A$, $n_B$, and $n_C$ are all relatively prime, Eve can use the Chinese Remainder Theorem to find $x$ such that $x \equiv y_A \bmod n_A$, $x \equiv y_B \bmod n_B$, and $x \equiv y_C \bmod n_C$. The CRT says that all such $x$ are congruent modulo $n_X$, so the $x$ that is less than $n_X$ must be $m^3$ ($m$ is less than any of the $n_{\{A|B|C\}}$, so $m^3$ is less than $n_X = n_A n_B n_C$). Therefore Eve can simply take the cube root (normal, not modular) of this value to recover $m$.

3. **(20 pts.) Secure PIN Entry**

   The display shows a random integer. The user increases it or decreases it (cycling around 0 using an UP or DOWN key on the keypad.) and presses ENTER to enter that digit as a PIN entry value. Note that this gives no information to an adversary about the value of the entry.

4. **(20 pts.) Firewalls and Reference Monitors**

   There are three properties for a reference monitor: non-bypassable, tamper-resistant, and verifiable. A firewall is non-bypassable if you verify that ALL network traffic from the outside to/from the inside is mediated by the firewall. It is tamper-resistant if it is designed to resist attacks against its hardware and software components (for example, if the software is contained in non-volatile memory). It is verifiable if we can formally verify that the design AND implementation are correct.

   In reality, verify the properties can be very difficult (if not impossible). We can test our network to determine if there are external access mechanisms that are not mediated by the firewall (e.g., modems or wireless access points). We can examine the software for potential vulnerabilities, but for a given hardware/software complexity, it may not be possible to determine whether there are bugs and whether they can be used to alter the firewalls behavior.

5. **(20 pts.) Intrusion Detection Systems**

   Rule-based intrusion detection uses a list of rules describing known attacks. It looks for matches between traffic and the rules, and is only effective at detecting known attacks. It is easier to explicitly

block a known exploit with rules, because we don't have to rely on the known exploit being statistically different from normal traffic.

Statistical anomaly detection looks for differences between normal behavior and attack behavior. It can be used to detect novel attacks. Statistical anomaly detection has the advantage that it can catch attacks that we did not explicitly write rules for.