Aughdon Breslin

Problem 1: Shared or forgotten keys?

1. Which two basic security properties should be considered in the design of a secure protocol solving the above problem and why these properties become relevant in this setting?
    a. Confidentiality and Integrity. They are communicating over an insecure channel, so they will need to ensure that their messages will be sufficiently encrypted to prevent outside parties from picking up on any information being discussed. Also, since they are communicating about a shared n-bit secret key, they need to make sure their message integrity remains intact so that they can be certain their communications from each other are accurate. If the integrity of the messages are compromised, Alice and Bob might believe the key is valid or secure when it has actually been tampered with.
2. This protocol does not satisfy either confidentiality or integrity. By doing x XOR y, the confidentiality is compromised, and there is nothing stopping a malicious party from changing the bits

Problem 2: Perfect or imperfect ciphers?

1. An attacker knows that a user's password is either 'abcd' or 'bedg'. Say the user encrypts his password using a Vigenere cipher, and the attacker sees a resulting ciphertext c. Show how the attacker can or cannot determine the user's password for period t = 1, 2, 3, or 4.
    a. t = 1: This is a Caesar Cipher, and the attacker can figure out the password by looking at the distance between the first two characters. 'ab' has a distance of 1, while 'be' has a distance of 3. The pattern of password 1 is [x, x+1, x+2, x+3] while the pattern of password two is [x, x+3, x+2, x+5].
    b. t = 2: This does not discern any additional info as to which password it could be. This is because the distance between the first and third, and the second and fourth characters for both passwords are the same. For example, characters 1 and 3, 'ac' and 'bd', both have a distance of 2, and characters 2 and 4, 'bd' and 'eg' also both have a distance of two. For an unknown shift, there is no way to distinguish the right password (aside from brute forcing the two guesses). The patterns are [x, y, x+2, y+2] for both passwords.
    c. t = 3: The first password follows the pattern [x, y, z, x+3], while the other text follows the pattern [x, y, z, x+5]. So by comparing the distance between the first and fourth characters, the attacker can discern the true password.
    d. t = 4: Because the key is now the length of the entire password, no additional information can be discerned, since both passwords follow the pattern [w, x, y, z]. Again this is still susceptible to a quick brute force of guessing between the two.
2. Show that the mono-alphabetic substitution cipher is trivial to break when the attacker launches a chosen-plaintext attack. How much chosen plaintext is needed to recover the

entire secret key? What is the shortest chosen single-message plaintext that you can find, which is a valid English message and would successfully recover the key? Finally, under which conditions, and why, is the mono-alphabetic substitution cipher perfectly secure (against a ciphertext-only attacker)?

a. A mono-alphabetic substitution cipher is trivial to break when the attacker launches a chosen-plaintext because any text with all of the alphabet will reveal the character mappings. The attacker can use the cipher text and map it back to the alphabet plaintext in order to figure out every single substitution.
b. A 25 character plaintext would be sufficient to reveal the mappings. For example, 'abcdefghijklmnopqrstuvwxy' would yield a ciphertext that could be mapped back to the alphabet, and then the missing character in the ciphertext would be mapped to 'z'.
c. After googling 'perfect pangram,' I found this message that uses all 26 English letters without redundancy: "Mr. Jock, TV quiz Ph. D., bags few lynx," from https://www.prdaily.com/16-clever-pangrams-for-word-lovers/.
d. A mono-alphabetic substitution cipher is perfectly secure if the probability of all mappings between the characters and their ciphertext are equally likely.

Problem 3: Crypt-analyze this!

1. Here are the 11 plaintext messages that were exchanged:

```
Testing testing can you read this
Yep I can read you perfectly well
Awesome one time pad is working
Yay we can make fun of Abrar now
I hope no student can read this
That would be quite embarrassing
Luckily OTP is perfectly secret
Didnt Abrar say there was a catch
Maybe yet I didnt pay attention
We should really listen to Abrar
Nah we are doing well without her
```

   a. I will have HW1.ipynb attached to show the process of my program, but it started by guessing a small phrase in one of the sentences and using an xor of two adjacent strings to see if any of them returned an intelligible string in response.
   b. 2 will also be explained via HW1.ipynb's ta_algo() function.
2. The key the TAs will be using in three weeks will be:
   ffe8144a63819ae4ba99c7549fa59776f5f8bbdd2841080f5ba87ce918c3578821

Problem 4: One more Crypto controversy…

1. Describe briefly the controversy related to Dual EC DRBG, by identifying various main stakeholders (organizations or companies rather than individuals), their involvement in the events, and their possibly conflicted goals.
    a. There exists quite a bit of controversy surrounding Dual EC DRBG because of its inclusion in NIST SP 800-90A, a publication that provides a seal of approval as a "Recommendation for Random Number Generation Using Deterministic Random Bit Generators." This was controversial because it had well-known weaknesses in the cryptographic security of the algorithm, such as the potential for the algorithm to have a kleptographic backdoor that the NSA and no one else knew about.
    b. According to the 2013 Reuters news article, in 2002, before NIST standardized Dual_EC_DRBG, NSA paid RSA Security $10 million in a secret deal to use Dual_EC_DRBG as the default in the RSA BSAFE cryptography library, which resulted in RSA Security becoming the most important distributor of the insecure algorithm. This makes both the NSA and RSA Security major stakeholders with conflicting goals than their intended purpose of solely providing security. The NSA is sacrificing the general public's security to ensure that it is capable of breaking into the messages of people using the algorithm, while the RSA Security is tempted by financial gain in order to allow this breach of security. Another stakeholder would be the ANSI group, who first saw the Dual_EC_DRBG algorithm, were aware of the mechanism to produce the backdoor, but did not step in to disable or publicize its vulnerability. Finally, the consumers are also a major stakeholder as they were the ones potentially misled into believing that the publication's recommendation meant Dual_EC_DRBG was secure when in reality their security would be compromised because of it.
2. Describe how one or more broad ethical concerns occur in the issue at hand, by clearly articulating what these concerns may be and how they are possibly impacted by different choices or related tradeoffs.
    a. One of the most critical ethical concerns in the issue at hand is for a respected publication and standard to be honest and trustworthy. The NSA sought to knowingly publish an insecure standard that they could use to their advantage, and the RSA Security elicited a $10 million secret deal to do this because of its position as a respected network security company, undermining its own reputation and betraying the consumers that believed in that reputation. By refusing the NSA an opportunity to breach consumer security, RSA Security could have prevented many security breaches by not making Dual_EC_DRBG the default CSPRNG in BSAFE. RSA Security also neglected to follow the ethical principle of implementing systems that are robustly and usable secure. This is because in practice, Dual_EC_DRBG was not cryptographically sound, as shown by a 2005 patent describing the working of an elliptic curve CSPRNG backdoor that was

identical to the potential backdoor in Dual_EC_DRBG. The NSA had discarded any form of a reputable perception from the public, being perceived as an unethical and invasive government program.

3. Describe some of the standard professional or societal codes of ethics that relate to the events, and what can the impact to our society be, when such codes are not applied.
    a. Some of the most prominent standard professional code of ethics according to the ACM's Code of Ethics that relate to this event are 1.3, 2.2, 2.5, and 3.1. These codes are as follows: 1.3 Be honest and trustworthy, 2.2 Maintain high standards of professional competence, conduct, and ethical practice, 2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks, and finally 3.1 Ensure that the public good is the central concern during all professional computing work. Firstly, a lack of honesty or trustworthiness from organizations with authority like the NSA undermines the public's whole perception of their governments. On the other hand, RSA Security's reputation is tarnished by unethical business decisions, violating ACM's Code of Ethics 2.2. They should not have published Dual_EC_DRBG as the default CSPRNG knowing its security flaw, and should not have followed the deal from the NSA. Thirdly, according to the New York Times, the backdoor was deliberately inserted by the NSA but had not been made known to the public that such a backdoor was possible. The NSA completely disregards many Codes of Ethics, showing traits of untrustworthy, unethical, secretive and self-serving practices that mislead the public and prioritize their own gains over the public's security as the central concern.