Anton Danylenko, Christian Paz
I pledge my honor that I have abided by the Stevens Honor System.

Problem 1)

1) The security properties necessary for this problem are confidentiality and integrity. Confidentiality is important because we don’t want other parties gaining access to either private key. We also want integrity to ensure that the private key does not change in transit.
2) This would violate confidentiality since an interceptor will have access to x and y, and $y = kb \oplus x$ -> $y \oplus x = (kb \oplus x) \oplus x$ -> $y \oplus x = kb \oplus 0$ -> $y \oplus x = kb$. Thus, the interceptor will have access to one of the private keys. Integrity is also violated because an interceptor can intercept x or y in transit and forward a different value to the receiver, ruining the protocol.

Problem 2)

1) An attacker cannot determine the user's password if the period is 4 because then each letter is shifted by a different amount- making it equal to the One Time Pad cipher, which is perfectly secure. For periods of 1, 2, and 3, however, we can calculate the difference between the first and second, second and fourth, and first and fourth letters respectively in the ciphertext. We can then compare this difference to the difference between respective letters in each of the two passwords and choose whichever password has the same difference. For example, if the period was 3 the first and fourth letters of the password would be shifted by the same amount- let’s say by 1. Then the ciphertext for p1 would be bcde and for p2 would be cfeh. In the first ciphertext the difference between the first and fourth letters would be 3 and for the second would be 5. This is the same in the original passwords so we can easily identify the right one.
2) Only 25 characters of plaintext would be needed because by process of elimination, the 26th character of the alphabet would be able to be determined. “Crwth vox zaps qi gym fjeld bunk” is a good contender for shortest plaintext needed because it is a perfect pangram and uses each letter of the alphabet only once. Perfect secrecy would be attained under the condition that the message is limited to one character. Otherwise, if the interceptor sees that the ciphertext is “xy” for example, they would already know that the plaintext is not two of the same letter, violating definition 2 of perfect secrecy- Pr[Enc(m) = c] = Pr[Enc(m’) = c].

Problem 3)

1) 'TheQuickBrownFoxJumpsOverLazyDog!'
   '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 Nicos now '
   'I hope no student can read this '
   'That would be quite embarrassing '
   'Luckily OTP is perfectly secret '

'Didnt Nicos say there was a catch'
'Maybe yet I didnt pay attention '
'We should really listen to Nicos '
'Nah we are doing well without him'

The key is TheQuickBrownFoxJumpsOverLazyDog!

Our strategy was to first use crib dragging with common words such as “this”, “the”, “you”, etc. We took the xor of two ciphertexts, which should be the same as the xor of those two respective messages. We then xor each of the common words against every slice of that cipher_xor and see if the result resembles english. One hit we had was with “ can “ with a result of “me on” in the 5th index of the ciphertext. We now knew that one of the messages had “ can “ in it and the other “me on” so we took the xor of each message and “ can “ to get two potential partial keys. We then xored the partial keys with every ciphertext to find the right partial key and also get the partial messages for each ciphertext. Once we had 11 partial messages, there were some obvious partial words that were revealed. We then expanded our key and continued the same two steps until the full messages were revealed and we got the full key.

2) **10/25 Key**
Received from the output of GetKeyByDaysPassed.py
167444343ab1bbe3dee24f02aaad94f3b98c3dcaeaf95a9eecaa18a67583bedd21

Problem 4)

1) One of the main weaknesses of the algorithm was that it gave those who knew about it (the United States government’s National Security Agency) a kleptographic backdoor to the algorithm. The NSA paid a company called RSA Security $10 million in a secret deal to use the DUA_EC_DRBG algorithm as the default in the RSA BSAFE cryptography library, so RSA Security was the main distributor of the insecure algorithm. However, the company denies that they knowingly colluded with the NSA to adopt a knowingly flawed algorithm claiming “we have never kept [our] relationship [with the NSA] a secret” (Wiki Article). The conflicting goals here is that RSA was doing this to make a profit, while the NSA was seemingly searching for a way to break SSL/TLS encryption that used this algorithm as a CSPRNG.
2) One of the main ethical concerns with the DUA_EC_DRBG algorithm is allowing the United States government (NSA) to have a backdoor (a bypass to normal authentication) to messages encrypted by this algorithm. Designing a cryptography algorithm with an intentional backdoor gives the NSA the ability to crack into encryption schemes which could be a major invasion of privacy and alludes to potential massive government surveillance. There is a cybersecurity framework made by the National Institute of Standards and Technology that offers security and privacy controls for software applications, cloud computing, and supply chain security. There is a direct conflict of interest here since the NSA has always directly influenced the standards that were created. DUAL_EC_DRBG at the time was significantly slower than other encryption

techniques described in the standard, and it was evident there was a huge weakness in this algorithm. People wondered why it was even included in the NIST standard, and uncoincidentally the NSA was the main supporter of this algorithm being included.

3) A societal code that directly relates to this is the fourth amendment. The fourth amendment protects American citizens from unreasonable searches and seizures. This includes but is not limited to their persons, houses, papers, etc. The NSA using the backdoor to crack this encryption algorithm to view messages without a warrant would be a major violation of the fourth amendment - the right to privacy. If this code was not applied, this would allow the government to tap into any conversations, search our homes at their discretion, and imminently allow the government to use overbearing surveillance on the American citizens. This exact scenario is already occurring in countries where the right to privacy does not exist like North Korea and China, and improved technology is allowing these governments to closely watch their citizens in a way that is more invasive than ever before.