Homework 3
Kaitlynn (Katie) Prescott
I pledge my honor that I have abided by the Stevens Honor System.
5 December 2018

Problem 1:

1. Brute Force Attack: Since every password has the same format, the keyspace is finite and relatively small, and Eve will be able to search through and find the correct password. If Eve knows the hash value of Alice's password, and she knows that the hash function is either SHA-1 or SHA-256, then she just needs to run a brute force algorithm, and she will be able to not only figure out the hash function used, but also Alice's password.
2. When user-specific salts are used, Eve would need to know Alice's salt in order to correctly discover her password. If she does not know Alice's salt before-hand, this would greatly increase the computational work Eve must do, and may make it infeasible.
3. If Eve knows and understands the birthday paradox, she knows it will be much easier to just match any password to it's hash, rather than trying to match it to Alice's in particular. Performing a birthday attack could make it much easier to crack Alice's password, as Eve won't have to go through as many permutations to find a collision.

Problem 2:

1. Honeywords improves password security because if the red server is compromised, the passwords, the password is still protected because the red server does not know the index of the correct password. If someone randomly inputs a password and there is no hit on the red server, then the red server rejects the login attempt, and if there is a hit but it is the incorrect index, then the blue server will reject the attempt.
2. (1) password1, (2) p@ssw0rd8, (3) p@$$w0rd5, (4) p@s$w0rd!5,
   (5) pa$sword#2, (6) #@ssw0rd!, (7) p@s$wo!d6, (8) pa%s#ord3, (9) p^$sw*rd9, (10) p&$s^0*d7
3. I would choose Blink-182 as the password, because it is a band from the 90s/2000s, and it contains a capital letter, a lower case letter, a number, and a special character. The rest of the passwords don't make sense because they do not have any real world meaning, since most people will have a real world meaning associated with their passwords so they do not forget.

Problem 3:

1. If Eve and Mallory use replay attacks, Mallory can change Bob's public key to an older key, that Bob revoked, and now Eve will be able to receive the new messages, and pass

them, verified by the signed certificate from Mallory, along to Bob's new public key, and she will be able to see every message sent to Bob.
2. If there is a one-day signing period, and no one resets their public key more than once a day, then each message and signed certificate will have the same time stamped date. You can verify messages by ensuring the certificate was signed on the same day as the message.
3. In order for time stamped signatures to be applied to DNSSEC, it would need to be regularly re-signed and distributed to secondary servers, otherwise, valid signatures can be rejected.

Problem 4:

1. Because they are using a semicolon to separate m1 from m2, Eve will be able to get a MAC tag on m1, and XOR it to a modified m2, and can get a valid MAC tag for a modified message. So Eve can get the MAC tag for "yes, thanks for the reminder!" and XOR the tag to a new message, perhaps "there is no HW4" and send it with a valid MAC tag.
2. Plain RSA is deterministic, and therefore not CPA secure, so Eve can use a chosen plaintext attack to discover what the messages say, and can learn what the topics on the final will be.
3. Someone can intercept and change the key exchange message, and replace the public key without detection. Without a MAC tag or timestamp signature, Bob would not be able to detect that someone intercepted the messages. Therefore, he should not send the exam solutions.

Problem 5:

1. If this quiz has fast statistics viewable by everyone, she can view what the most common answer is for each question, and since everyone else has studied, it will be more reliable than guessing. Also, because new uploads are allowed and it just overwrites the existing file, she can go back and change her answers after she finishes, ensuring she gets the correct answer.
2. Because plain RSA is deterministic, the cipher text for the same plaintexts will be the same. This will allow BestCloudStore to encrypt a file, search for the ciphertext in their system, and if it exists already, it can save the current file as a pointer to the file they already have in their system, thus eliminating any duplicate files.
3. ElGamal is not deterministic, so, while it may be more secure than plain RSA, it will not allow for deduplication, because the encryption of a file will not be the same every time.