Assignment 2

1)

a. Bob's mistake was asking Alice to authenticate her secret key using the same 128-bit secret key. That would make K xor M = 0 and Bob didn't have her secret key to authenticate either (assuming he refused her encrypted msg with using his public encryption key). Bob and Alice should exchange secret key for HMAC using Diffie-Hellman. After both parties obtained secret key, Alice would send encrypted AES in CBC mode key using Bob's public key and HMAC to authenticate Alice's identity.

b. Bob's problem was only sending the certificate to Alice. He should send the certificate along with both public keys and signed version of the public encryption key. Alice would check the signature on the certificate using 256-bit ECC public key and then use the certificate to verify Bob's public encryption key.

c. Bob's problem is requiring Alice to hash and salt her password. If users are using the same salt and same password, the attacker can precompute hash table to figure out her password. Bob should ask Alice to encrypt her username and password using 128-bit AES then Bob would decrypt it and hash her password with a unique salt to server database.

d. Bob's problem is using AES to encrypt passwords for secured storage. Bob should use hash with unique salt to store users' passwords more secure.

2)

a. Superfish uses keybridging to prevent your browsers from thinking that it made a complete encrypted connection (HTTPS connection). When your browser connects to a secured webpage, the content from the webpage has been decrypted by Superfish's filters. Superfish is now able to alter the contents of a web page. After that, Superfish encrypts the data again that makes your browser think that it is end-to-end encrypted connection.

b. Since Superfish used the same signing key in every laptop computer, the attacker would simply obtain signing key and sign their own public key to generate valid certificate. Users (victims) could verify and allow browser to access attacker's website.

c. User access to well-known website such as google.com because they are encrypted connection and issued by Google itself. Click on the lock on the left of the URL and click on certificate (Valid). The pop-up shows certificate information issued to google.com. Users need to carefully check line "Issued by" that is not from Superfish. Otherwise, you are infected by Superfish.