CSE 565 Solution to Homework 2

1. (12 points) When the CFB encryption mode is used as a stream cipher, we select r most significant bits of the block cipher's output to form an r-bit cipherblock, which is consequently used as the feedback to the next iteration of the algorithm. The shift register is updated to keep $n-r$ least significant bits of the register's content from the previous iteration, which are combined with the feedback. To use this operation in the formulas, we can either introduce new notation for selecting a certain number of least significant bits of a buffer. For example, we could use notation $L_k(a)$ to select k least significant bits of a. Alternatively, we could use the left shift operation $\ll$ to update the shift register. If we denote by $a \ll k$ logical left shift by k bits, then the shift register update can be written as $(a \ll r) + b$, where a denotes the n-bit content of the shift register at the previous iteration and b denotes the r-bit feedback. In the formulas below we use the former notation.

   For CFB encryption of r-bit message blocks $m_1, m_2, \ldots$, we obtain: set I_1 to be a randomly chosen n-bit IV and form r-bit cipherblocks as $c_i = S_r(E_k(I_i)) \oplus m_i$, $I_{i+1} = L_{n-r}(I_i)||c_i$. The transmitted ciphertext is $IV, c_1, c_2, \ldots$. To decrypt, one sets $I_1 = IV$ and computes $m_i = S_r(E_k(I_i)) \oplus c_i$, $I_{i+1} = L_{n-r}(I_i)||c_i$.

   For the OFB mode, the change is minor. We use r bits of the block cipher's output instead of a cipherblock and for encryption obtain $t_i = S_r(E_k(I_i))$, $c_i = t_i \oplus m_i$, $I_{i+1} = L_{n-r}(I_i)||t_i$. Similarly, decryption is performed by setting $I_1 = IV$ and computing $t_i = S_r(E_k(I_i))$, $m_i = t_i \oplus c_i$, $I_{i+1} = L_{n-r}(I_i)||t_i$.

2. (10 points each; 20 points total)

   (a) Assuming that Alice chose a good hash function for long-term security, a judge should believe her claim. That is, the second preimage resistance property of the hash function assures that after the newspaper was published Alice would not be able to create a new document to match the published digest. Assuming Alice's hash function has second preimage resistance property with sufficient output length n so that performing a significant fraction of 2^n hashings was not feasible during the 15 years, the community should believe her claim.

   (b) Signature schemes achieve a different security objective and are not the appropriate tool in this case. The answer to this question depends on the signature scheme used and what exactly was published. That is, if the signature was published without the corresponding public verification key, her claim is unlikely to be believed. A signature is valid with respect to a fixed known key, and nothing is guaranteed when it is being verified using a different key. In fact, for a number of existing algorithms, the same signature can be a valid signature on different messages under different public keys. If the public key was published in the paper as well, then trustworthiness of the claim depends on the signature algorithm. That is, most signature algorithms use a hash-then-sign paradigm, and finding another message that will pass the verification process won't be feasible, assuming a hash function with adequate security properties was used. (A signature on a document is also not guarantees to provide confidentiality of the document. My signature algorithms, however, sufficiently protect the message and we assume that Alice wouldn't choose a signature scheme that leaks her document.)

3. (18 points total)

(a) (10 points) Eve chooses one public-private key pair (pk_1, sk_1) and replaces Alice's public key on the server with pk_1. Eve also chooses another public-private key pair (pk_2, sk_2) and replaces Bob's public key with pk_2.

When Alice wants to send a message to Bob, she retrieves the public key pk_2 and encrypts her message using it. Eve will then intercept the message, decrypt it, re-encrypt with Bob's true public key and send it to Bob (pretending to be Alice). Similarly, when Bob wants to send a message to Alice, he encrypts it with key pk_1, and Eve needs to intercept and re-encrypt the message using Alice's true key.

Public key encryption does not provide sender authentication, so Eve can always forge messages from either, without modifying data stored on the server.

(b) (8 points) Alice can detect that her public key stored on the server is incorrect by either (i) encrypting message to herself with the public key stored on the server and trying to decrypt it with her private key or (ii) applying a data integrity mechanism to the key stored on the server and verifying the authenticity of the key. She should also keep a copy of the true public key on her trusted machine or trusted storage (such as a CD) and can compare what is stored on the server with the key that she has. Bob can perform the same procedures to verify the authenticity of his key stored on the server.

4. (20 points total; 4 points each) Answers vary.

In general, the banking industry takes computer security more seriously than many other sectors and banks are more likely to implement the recommended protection mechanisms than other companies. Break-ins nevertheless take place, with small banks (who often rely on an external company for this protection) being more vulnerable.