Cryptography and Security 2017

Solution Sheet 8

Solution 1 Attack Against the OFB Mode

1. The OFB mode is nothing but a one-time pad with a sequence generated from the IV and the secret key. If they are both fixed, the sequence is always the same as it is independent from the plaintext. Therefore, from a known plaintext attack with only one known message, we can recover the key stream and decrypt any new ciphertext (of the same length or shorter).
2. The CFB mode is stronger against this issue, except for the first block. The first encrypted block is equal to the first plaintext block XORed with a value generated from IV and from the key only. The next values in the sequence depend on the plaintext. Similarly, note that if two plaintexts are equal on their first n blocks, the knowledge of one of the plaintexts allows to recover the $(n+1)$th block of the other plaintext.
3. The CBC mode is not vulnerable to this kind of attack.

Solution 2 RC4 Biases

1. It is $\frac{1}{N} \times \frac{N-2}{N-1}$ with $N = 256$.
2. Let $S(1) = x$ and $S(x) = y$ initially. At the first iteration, i is set to 1, j is set to x, and $S(1)$ and $S(x)$ are exchanged. Their values become y and x respectively. Then, i is set to 2, j is set to x again, and $S(2)$ and $S(x)$ are exchanged. Their values become x and 0 respectively. The output is $S(x)$ which is 0.
3. Clearly, $p = \frac{1}{N} \times \frac{N-2}{N-1} + \frac{1}{N}(1 - \frac{1}{N}\frac{N-2}{N-1}) \approx \frac{2}{N}$. This is twice that what we should expect. This is a deviant property which should be avoided.

Solution 3 Attack on 2K-3DES

This exercise is based on "On the security of multiple encryption" by Merkle and Hellman, Communications of the ACM, Vol. 24(7), July 1981.

1. Blocks have 64 bits. The key has 56 effective bits.

   With a single plaintext-ciphertext pair (x, y) with a known plaintext, it is enough to characterize the correct key as no wrong key shall be consistent with probability $\left(1 - 2^{-64}\right)^{2^{56}} \approx e^{-2^{-8}}$ which is very close to 1. The average complexity is of 2^{55} trials with a small memory (just enough to store the data and a counter).
2. We now need two pairs (x_i, y_i), $i = 1, 2$ to characterize the correct key uniquely. With 2 known plaintexts, we prepare a dictionary of 2^{56} records $(\mathsf{DES}_b^{-1}(y_1), b)$ for all b. Records are sorted by their first two values. The dictionary takes 8×2^{56} bytes. There would be tricks to shrink it a bit but the order of magnitude should stay 2^{56}. Then, for all a we compute $(\mathsf{DES}_a(x_1))$ and check if this is in the dictionary. When it is, b is given by the dictionary and we check if $y_2 = \mathsf{DES}_b\left(\mathsf{DES}_a(x_2)\right)$. If it matches, then $K_1 = a$ and $K_2 = b$ is the correct key. The time complexity consists of 4×2^{56} DES encryptions. Again, there would be tricks to reduce it a bit but the order of magnitude should stay 2^{56}.

3. For each a we compute $x = \mathsf{DES}_a^{-1}(0)$ and use x as a chosen plaintext. We obtain y. Then, we check if $\mathsf{DES}_a^{-1}(y)$ is in the dictionary. If it is, it means that $\mathsf{DES}_a^{-1}(y) = \mathsf{DES}_b^{-1}(0)$ for some b and it gives b. Clearly, x encrypts to y with key (a, b). With a previous plaintext-ciphertext pair we can check if this key is correct. Clearly, when a becomes equal to K_1 (which would happen after an average number of trials equal to 2^{55}), this attack recovers K_2. So, it works with a number of DES operations equal to 3×2^{55}, 2^{55} chosen plaintexts, and a dictionary of 2^{56} entries.