

Problem Set 2

Due at the *start* of class, Wednesday, March 5, 2008.

Problem 1. [5 points] What fraction of the total number of possible permutations does DES use?

Problem 2. [10 points] Prove using induction that the output of the i th round of DES decryption is the same as the output of the $(16 - i)$ th round of DES encryption. We did the base case in class, but you should repeat it as part of your proof for completeness.

Problem 3. (Mao 7.1) [10 points] In cipher block chaining (CBC) mode of operation for a block cipher, if the decryption of a received ciphertext “has the right padding,” should this suffice as a sufficient check of the plaintext’s integrity? Explain. How about when using ciphertext feedback (CFB) mode?

Problem 4. (Stallings and Brown 19.3) [10 points] For any block cipher, the fact that it is a nonlinear function is crucial to its security. To see this, suppose that we have a linear block cipher EL that encrypts 128-bit blocks of plaintext into 128-bit blocks of ciphertext (like AES does). Let $EL_K(m)$ denote encryption of 128-bit message m under key K (its bit length is irrelevant). Then, linearity means that for all $m_1, m_2 \in \{0, 1\}^{128}$,

$$EL_K(m_1 \oplus m_2) = EL_K(m_1) \oplus EL_K(m_2).$$

Describe how this property enables an adversary to decrypt any target ciphertext without knowledge of the secret key K using a chosen-ciphertext attack with only 128 chosen ciphertexts.

In a chosen-ciphertext attack, the adversary obtains the decryption of each chosen ciphertext it submits (other than the one it’s trying to break). The adversary can submit the ciphertexts in any order and decide what to submit next based on the results of all previously submitted ciphertexts.

Problem 5. So far in most of our discussions of block ciphers we have focused on the length k of the key K . In the best case, when the attacker is forced to conduct an exhaustive key search, we say the *effective key-length* is equal to $k - 1$. On the other hand, in the case of 2DES we saw the effective key-length may be less than k (due to the meet in the middle attack in that case). However, the block-length n (64 bits for DES) also impacts security. AES, the replacement for DES, has a larger (minimum) key-length of $k = 128$ and a larger block-length of $n = 128$. Consider a block cipher called SBS that has $n = 8$ and $k = 56$ (the details of how it works are irrelevant).

a) [6 points] Do you think SBS is more secure, less secure, or roughly as secure as DES? Why? (Try to reason about SBS’s effective key-length: is it roughly 56 or considerably less?)

b) [2 points] What can you infer/conclude about the relation of n, k , and the effective key-length?

c) [2 points] What might be a good lower-bound for n in terms of k ?

Problem 6. [10 points] One problem with ciphertext feedback (CFB) mode (that OFB/CTR modes share) is the computation overhead. To encrypt each r -bit message fragment requires encrypting an entire block, i.e. the contents of the n -bit “input register”. Suppose we use up all of the output bits from the first block encryption before updating the input register. In other words, if for example $r = n/2$, m_1 is XORed with the left-most r bits of $O_1 = \text{Enc}_K(IV)$, m_2 with the right-most r bits of O_1 , m_3 with the left-most r bits of $O_2 = \text{Enc}_K(c_1c_2)$ (the block-encryption of the concatenation of c_1 and c_2), etc. Why might this be less secure than CFB mode? Feel free to consult (and cite!) any external resources.