Exercise sheet 5, 15 December 2016

You can find the authoritative description of DES at `http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf`

1. Use Shamir's secret sharing to share $s = 5$ over $\mathbb{F}_{103}$ in an 3 out of 5 fashion. You don't need to compute the shares for verification, i.e. the $g^{f(j)}$. Verify for two sets of 3 users that you can recover the secret.

2. Let the RSA secret key d be shared in a t out of n fashion. Show how to do RSA decryption using shares locally, i.e. without recovering the secret s.

3. Let the DH secret a be shared in a t out of n fashion. Show how to compute g^{ab} given g^b and the shares, without recomputing s, i.e. using the shares locally.

4. Take S_5 and compute $S_5(x_1) \oplus S_5(x_2)$ and compare the result with $S_5(x_1 \oplus x_2)$ for the following values:

   (a) $x_1 = (000000), x_2 = (100000)$

   (b) $x_1 = (111111), x_2 = (000001)$

   (c) $x_1 = (000000), x_2 = (101010)$

5. Compute the first subkey if the 56-bit key consists of 56 zeros.

6. Compute the output of the first round (i.e. include the initial permutation, the split into left and right, the function f, the xor and the swap) when the input is the all-zero string and the key is 56 zeros.

7. Compute the output of the first round (i.e. include the initial permutation, the split into left and right, the function f, the xor and the swap) when the input is the all-zero string with the rightmost bit replaced by 1 and the key is 56 zeros. Do not forget the initial permutation.

8. The Electronic-Code-Book (ECB) mode encrypts long texts by chopping them into blocks matching the input size of the block cipher (possibly after padding to match the length) and encrypting them individually. We've seen that this is a bad idea. The Cipher-Block-Chaining (CBC) mode avoids this problem by linking the encryption of the present block with the ciphertext of the previous block; the encryption of the first block uses an Initialization Vector (IV) instead of the ciphertext block. Encryption then works as follows:
   $c_1 = \mathrm{Enc}_k(m_1 \oplus IV)$,
   $c_i = \mathrm{Enc}_k(m_i \oplus c_{i-1})$ for $i \geq 2$.
   Show how to decrypt $(IV, c_1, c_2, c_3, \ldots)$.

9. Check out
   `http://blog.fortinet.com/post/angecryption-at-insomni-hack`.

10. Read up on the POODLE attack (e.g `https://en.wikipedia.org/wiki/POODLE` and references).