Security I - Supervision 1

March 2013

a. What is perfect secrecy? Indistinguishably in the presence of an eavesdropper? CPA security? CCA security?

b. Solve following equations for $X$ in a finite field $GF(p)$ where $p = 11$

- $X = 8 + 7$
- $X = 4 - 10$
- $X = 5 \cdot 7$
- $3 \cdot X = 1$
- $3 \cdot X = 8$

Perform the following operations in a finite field $GF(2^4)$ where the modulo polynomial is $x^4 + x + 1$ (10011)

- $1010 \oplus 0011 \ (x^3 + x) \oplus (x + 1))$
- $1010 \odot 0011 \ (x^3 + x) \odot (x + 1))$
- $1101 \otimes 1001 \ ((x^3 + x^2 + 1) \otimes (x^3 + 1))$

c. How many different functions are there that map $n$-bit string to $n$-bit string ($F : \{0,1\}^n \rightarrow \{0,1\}^n$)? How about permutation $P : \{0,1\}^n \leftrightarrow \{0,1\}^n$?

Note that a block cipher is just a (tiny) subset of these permutations.

d. How do you distinguish a Feistel cipher from a random function if it has only (a) one round, (b) two rounds?

Use the setup on page 34 of the lecture notes, where you can submit arbitrary encryption queries to a black box. The black box implements either the Feistel cipher in question with an unknown key or a random permutation. Your job is to find out which one it implements.

e. What is Kerckhoffs’ principle?

What happens to the ciphertext block if all bits in both the key and plaintext block of DES are inverted?

\[ \text{1it’s NOT a permutation of bits within the block!} \]
f. Explain in diagrams how each of the modes (ECB, CBC, CFB, OFB and CTR) encrypts/decrypts. Which modes can parallelise its encryption and/or decryption?  

Suppose there are $n$ ciphertext blocks but one bit in the $n/2^{th}$ block is flipped, how many plaintext bits are expected to be flipped in each of these modes? Assume the underlying block cipher has a block length of 128 bits.

g. Using a given pseudo-random function $F : \{0, 1\}^{100} \rightarrow \{0, 1\}^{100}$, construct a pseudo-random permutation $F : \{0, 1\}^{300} \rightarrow \{0, 1\}^{300}$ by extending the Feistel principle appropriately.

h. You opponent has invented a new stream cipher mode of operation for DES. He thinks that OFB could be improved by feeding back into the key port rather than the data port of the DES chip. He therefore sets $R_0 = K$ and generates the key stream by $R_{i+1} = E_{R_i}(R_0)$. Is this better or worse than OFB?

i. A programmer wants to use CBC in order to protect both the integrity and confidentiality of network packets. She attaches a block of zero bits $P_{n+1}$ to the end of the plaintext as redundancy, then encrypts with CBC. At the receiving end, she verifies that the added redundant bits are after CBC decryption still all zero. Does this test ensure the integrity of the transferred message?

j. In slide 52 you were shown CBC with random IV as a type of randomized encryption. Explain: Why do we need randomized encryption. What are the advantages vs non-randomized encryption?

k. What happens if we use CBC with an unknown but predictable IV? Hint: think of the attack models presented in slide 11.

l. In CTR (see slide 57), why does the offset $O$ need to be chosen randomly?

m. Decipher the shift cipher text:

```
LUXDZNUAMNDODJUDTUZDGYQDLUXDGOJDCDKDTKJDOZ.
```