

1. A Hill cipher is defined over Galois field $GF(2^4)$ with polynomial $x^4 + x + 1$. The encryption key is the 2×2 -matrix

$$\begin{pmatrix} x^2 & 1 \\ 1 & x+1 \end{pmatrix}, \text{ or using bit notation } \begin{pmatrix} 0100 & 0001 \\ 0001 & 0011 \end{pmatrix}.$$

- a) (3 pts) Compute the encryption of the word $(x^2, x+1) = (0100, 0011)$.
- b) (3 pts) Compute the decryption key.
2. Alice and Bob use CBC encryption. The plaintext is a sequence of blocks P_1, P_2, \dots, P_t and the corresponding ciphertext blocks sent by Alice to Bob are C_1, C_2, \dots, C_t . Bob receives ciphertext blocks C'_1, C'_2, \dots, C'_t , where exactly one ciphertext block C'_j has an error, where $1 \leq j < t$. Then $C'_i = C_i$ for all $i = 1, 2, \dots, t, i \neq j$, and $C'_j \neq C_j$.
- a) (3 pts) Show that after decryption by Bob exactly two plaintext blocks are erroneous. What are the indices of the erroneous plaintext blocks?
- b) (3 pts) How the erroneous plaintext blocks differ from the original?
3. Sun Tsu was a Chinese mathematician, sometime between the third to fifth century AD. To illustrate the Chinese Remainder Theorem he used an example

$$x \equiv 2 \pmod{3}$$

$$x \equiv 3 \pmod{5}$$

$$x \equiv 2 \pmod{7}$$

- a) (3 pts) Solve for $x \bmod 105$.
- b) (3 pts) RSA can also be defined for a modulus n which is a product of three different primes. Similarly as in the usual case, the encryption exponent e and the decryption exponent d must satisfy
- $$ed \equiv 1 \pmod{\phi(n)}.$$
- For $n = 105$ and $e = 7$ compute d .

4. (6 pts) Explain the Man-in-the-Middle Attack on the basic (unauthenticated) Diffie-Hellman key exchange protocol.
5. (6 pts) Assume that we have two number generators as black boxes. Both generators output 64-bit numbers. One box contains a Counter Mode PRNG using Triple-DES encryption as E_K and with a counter of length 64 bits. The second box contains a true random number generator. The boxes look exactly the same, and the task is to determine which one is the true RNG just by examining the output of the generators. After both generators have produced about 2^{32} numbers, one has about 50% chance of being able to distinguish the generators. Explain why.