Cryptographic Engineering
Spring Term 2018

Homework Assignment 01:

1. Illustrate the computation of $\gcd(5270760, 50820)$ using factorization.
2. Illustrate the computation of $\gcd(651, 112)$ using the EA.
3. Illustrate the computation of $25^{-1} \pmod{128}$ using the EEA.
4. Compute $\phi(500)$.
5. Compute $25^{-1} \pmod{101}$ using Fermat's theorem.
6. Compute $23^{-1} \pmod{100}$ using Euler's theorem.
7. Compute $a+b \pmod{n}$, $a-b \pmod{n}$, $a \cdot b \pmod{n}$ for $a = 10$, $b = 7$, $n = 16$ in least positive and least magnitude representation.
8. Illustrate the computation of $m^{173} \pmod{n}$ using the binary method of modular exponentiation.
9. Given the moduli set $(7, 11, 13, 16)$ and the remainders $(1, 2, 3, 4)$ of the number x, compute x using the CRA.
10. Given the moduli set $(7, 11, 13, 16)$ and the remainders $(4, 3, 2, 1)$ of the number x, compute x using the MRC.
11. List all primitive elements $\mathcal{Z}_{101}^*$.
12. List the elements of $\mathcal{Z}_{101}^*$ which are of order 10.
13. Compute $a+b$ and, $a \cdot b$ in GF(2^7) using the irreducible $p(\alpha) = \alpha^7+\alpha+1$ such that $a = \alpha^5 + \alpha^3 + \alpha$ and $b = \alpha^6 + \alpha^4 + 1$.
14. The AES algorithm uses the field GF(2^8) with the irreducible polynomial $p(\alpha) = \alpha^8 + \alpha^4 + \alpha^3 + \alpha + 1$. Compute $a \cdot b$ in GF(2^8) given $a = \alpha^7 + \alpha$ and $b = \alpha^7 + 1$
15. The MixedColumn sub-round of the AES uses the matrix vector computation
$$\begin{bmatrix} \alpha & \alpha+1 & 1 & 1 \\ 1 & \alpha & \alpha+1 & 1 \\ 1 & 1 & \alpha & \alpha+1 \\ \alpha+1 & 1 & 1 & \alpha \end{bmatrix} \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \end{bmatrix}$$
for a given column vector of the state $[s_1, s_2, s_3, s_4]^T$. Perform this computation GF(2^8) for
$$\begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \end{bmatrix} == \begin{bmatrix} \alpha^6 + \alpha \\ \alpha^5 + \alpha^4 \\ \alpha^7 + \alpha^3 \\ \alpha^4 + \alpha^3 \end{bmatrix}$$
16. The SubByte table the AES involves the inversion of an element of in GF(2^8). Compute a^{-1} for $a = \alpha^7 + \alpha^3$.