King Fahd University of Petroleum and Minerals
College of Computer Sciences and Engineering
**Department of Computer Engineering**

**ICS 555 – Data Security and Encryption (T162)**

**Homework # 02 (due date & time: Wednesday 29/03/2017 during class period)**

**Problem # 1 – 10 points:** Compute the following $A(x) \cdot B(x)$ mod $P(x)$ in $GF(2^4)$, where $A(x) = x^2+1$, $B(x) = x^3+x^2+1$, and $P(x) = x^4+x+1$ being the irreducible polynomial.

**Problem # 2 – 20 points:** The following table contains a list of all multiplicative inverses for this field. As such, compute $(x^4+x+1)/(x^7+x^6+x^3+x^2)$ in $GF(2^8)$, where the irreducible polynomial is the one used by AES, $P(x)=x^8+x^4+x^3+x+1$.

| X \ Y | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 00 | 01 | 8D | F6 | CB | 52 | 7B | D1 | E8 | 4F | 29 | C0 | B0 | E1 | E5 | C7 |
| 1 | 74 | B4 | AA | 4B | 99 | 2B | 60 | 5F | 58 | 3F | FD | CC | FF | 40 | EE | B2 |
| 2 | 3A | 6E | 5A | F1 | 55 | 4D | A8 | C9 | C1 | 0A | 98 | 15 | 30 | 44 | A2 | C2 |
| 3 | 2C | 45 | 92 | 6C | F3 | 39 | 66 | 42 | F2 | 35 | 20 | 6F | 77 | BB | 59 | 19 |
| 4 | 1D | FE | 37 | 67 | 2D | 31 | F5 | 69 | A7 | 64 | AB | 13 | 54 | 25 | E9 | 09 |
| 5 | ED | 5C | 05 | CA | 4C | 24 | 87 | BF | 18 | 3E | 22 | F0 | 51 | EC | 61 | 17 |
| 6 | 16 | 5E | AF | D3 | 49 | A6 | 36 | 43 | F4 | 47 | 91 | DF | 33 | 93 | 21 | 3B |
| 7 | 79 | B7 | 97 | 85 | 10 | B5 | BA | 3C | B6 | 70 | D0 | 06 | A1 | FA | 81 | 82 |
| 8 | 83 | 7E | 7F | 80 | 96 | 73 | BE | 56 | 9B | 9E | 95 | D9 | F7 | 02 | B9 | A4 |
| 9 | DE | 6A | 32 | 6D | D8 | 8A | 84 | 72 | 2A | 14 | 9F | 88 | F9 | DC | 89 | 9A |
| A | FB | 7C | 2E | C3 | 8F | B8 | 65 | 48 | 26 | C8 | 12 | 4A | CE | E7 | D2 | 62 |
| B | 0C | E0 | 1F | EF | 11 | 75 | 78 | 71 | A5 | 8E | 76 | 3D | BD | BC | 86 | 57 |
| C | 0B | 28 | 2F | A3 | DA | D4 | E4 | 0F | A9 | 27 | 53 | 04 | 1B | FC | AC | E6 |
| D | 7A | 07 | AE | 63 | C5 | DB | E2 | EA | 94 | 8B | C4 | D5 | 9D | F8 | 90 | 6B |
| E | B1 | 0D | D6 | EB | C6 | 0E | CF | AD | 08 | 4E | D7 | E3 | 5D | 50 | 1E | B3 |
| F | 5B | 23 | 38 | 34 | 68 | 46 | 03 | 8C | DD | 9C | 7D | A0 | CD | 1A | 41 | 1C |

**Problem # 3 – 10 points:** Assume that (**`E0,B4,52,AE`**) is a column of the input state to the **`MixColumn`** step of AES, find the 2nd element of the corresponding column of the output state of the **`MixColumn`** step.

**Problem # 4 – 20 points; 10 points each:** Consider the field $GF(2^4)$ with $P(x)=x^4+x+1$ being the irreducible polynomial. Find the inverses for each of $A(x) = x$ and $B(x) = x^2 + x$ by applying the Extended Euclidean algorithm for polynomials. Verify your answer by multiplying the inverses you determined by $A$ and $B$, respectively.

**Problem # 5 – 10 points:** Using the Extended Euclidean algorithm, find the multiplicative inverse of 19 mod 999.

**Problem # 6 – 20 points; 10 points each:** Compute the inverse $a^{-1}$ mod $n$ with Fermat's Theorem (if applicable) or Euler's Theorem:

1. $a = 5$, $n = 12$
2. $a = 6$, $n = 13$

**Problem # 7 – 10 points:** Use Euler's Theorem to compute $((33^{71} + 285^{43}) \cdot (143^{20} + 150^{61}))$ mod 7.