Coding and cryptography
Assignment 3

Due **11:00am Tuesday 4th April 2023**

- This assignment is *compulsory*: in order to pass the course you need to score at least 55% on both this assignment and the written exam.
- *You have to do this assignment on your own.* You may not discuss with other people.
- You are not allowed to use computer programs, etc.
- This assignment must be handed in as a single pdf file on canvas. If the pdf is a scan, please make sure the text is readable. Photographs are highly discouraged.
- If you have any questions, email Ronen at `r.z.brilleslijper@vu.nl` .

Let $F = GF(2^6)$ be $K[x]$ modulo the primitive polynomial $h(x) = 1 + x + x^3 + x^4 + x^6$, and let α be the class of x. The table below gives the binary representation of $0, 1, \alpha, \alpha^2, \ldots, \alpha^{62}$.

1. Using (clever and efficient) calculations, check from scratch that the entries in the table for α^{13} and α^{26} are correct.

Let $\beta = \alpha^7$ so that $1, \beta, \ldots, \beta^8$ are all distinct and $\beta^9 = 1$. Let

$$g(x) = (\beta + x)(\beta^2 + x)(\beta^3 + x)(\beta^4 + x)\,.$$

Then $g(x)$ is the generator polynomial of a Reed-Solomon code $RS(9, 5)$ over F with length $n = 9$ and distance 5. (Note that this is the general case of Reed-Solomon codes where β is not necessarily a primitive element of $GF(2^6)$.) In problem 2 below, you have to use the algorithms treated in the course to decide if a received word w can or cannot be corrected to a codeword v by correcting at most two errors, and carry out this correction where it is possible.

2a. Compute the error locator polynomial $\sigma(z)$ using the first method (as in Section 6.3) if the syndromes of a received word w_1 are $s_1 = \alpha^{37}$, $s_2 = \alpha^{23}$, $s_3 = \alpha^9$ and $s_4 = \alpha^{58}$. Determine if w_1 can be corrected, and, if so, carry out this correction.

2b. Compute the error locator polynomial $\sigma(z)$ using the first method (as in Section 6.3) if the syndromes of w_2 are $s_1 = \alpha^{53}$, $s_2 = 0$, $s_3 = \alpha^{32}$ and $s_4 = \alpha^{62}$. Determine if w_2 can be corrected, and, if so, carry out this correction.

2c. Use the transform method (as in Section 6.4) to determine if w_3 can be corrected, and, if so, carry out this correction, if w_3 has syndromes $s_1 = \alpha^{41}$, $s_2 = \alpha^{62}$, $s_3 = \alpha^{20}$ and $s_4 = \alpha^{41}$.

3. Decrypt the message $(2, 23)$ under ElGamal with $p = 41$, $\alpha = 7$, and private key $a = 13$.

000000	0	001001	α^{15}	100110	α^{31}	010111	α^{47}
100000	1	110010	α^{16}	010011	α^{32}	111101	α^{48}
010000	α	011001	α^{17}	111111	α^{33}	101000	α^{49}
001000	α^2	111010	α^{18}	101001	α^{34}	010100	α^{50}
000100	α^3	011101	α^{19}	100010	α^{35}	001010	α^{51}
000010	α^4	111000	α^{20}	010001	α^{36}	000101	α^{52}
000001	α^5	011100	α^{21}	111110	α^{37}	110100	α^{53}
110110	α^6	001110	α^{22}	011111	α^{38}	011010	α^{54}
011011	α^7	000111	α^{23}	111001	α^{39}	001101	α^{55}
111011	α^8	110101	α^{24}	101010	α^{40}	110000	α^{56}
101011	α^9	101100	α^{25}	010101	α^{41}	011000	α^{57}
100011	α^{10}	010110	α^{26}	111100	α^{42}	001100	α^{58}
100111	α^{11}	001011	α^{27}	011110	α^{43}	000110	α^{59}
100101	α^{12}	110011	α^{28}	001111	α^{44}	000011	α^{60}
100100	α^{13}	101111	α^{29}	110001	α^{45}	110111	α^{61}
010010	α^{14}	100001	α^{30}	101110	α^{46}	101101	α^{62}

Distribution of points: 1: 4 2a: 8 2b: 12 2c: 12 3: 4 **Assignment grade: Total/4**