Crib of 4F5 exam 2018

JS

May 18, 2018

1. (a) We compute

$$\begin{aligned} R_9(17^{17}+17) &= R_9\left(R_9(17)^{17}+R_9(17)\right) \\ &= R_9\left(8\cdot(8^2)^8+8\right) \\ &= R_9\left(R_9(8)\cdot R_9((R_9(64))^8)+8\right) \\ &= R_9(8\cdot 1^8+8)=7. \end{aligned}$$

(b) Let $n=2k+1$, then

$$\begin{aligned} R_{11}(10^n+1) &= R_{11}\left(R_{11}(R_{11}(10)(R_{11}(10^2)^k))+1\right) \\ &= R_{11}(10\cdot 1^k+1)=0, \end{aligned}$$

hence 11 divides 10^n+1.

(c) We write

$$\begin{aligned} 554433221122334455 &= 55\times 10^{16}+44\times 10^{14}+33\times 10^{12}+\ldots+33\times 10^4+44\times 10^2+55 \\ &= 11(5\times 10^{16}+4\times 10^{14}+\ldots+4\times 10^2+5\times 10^0) \\ &= 11\times 50403020102030405 \end{aligned}$$

(d) We use Stein's algorithm as follows

$$\begin{aligned} \gcd(138600,305760) &= 2\gcd(69300,152880)=4\gcd(34650,76440)=8\gcd(17325,38220) \\ &= 8\gcd(17325,19110)=8\gcd(17325,9555)=8\gcd(3885,9555) \\ &= 8\gcd(3885,2835)=8\gcd(1050,2835)=8\gcd(525,2835) \\ &= 8\gcd(525,1155)=8\gcd(525,315)=8\gcd(105,315) \\ &= 8\gcd(105,105)=8\times 105=840. \end{aligned}$$

(e) $\gcd\left(\frac{a}{c},\frac{b}{c}\right)=\frac{1}{c}\gcd(a,b)$

(f) (i) This algebraic system is a monoid because 0 has no multiplicative inverse.

(ii) $k=2,6$ both divide the order 7560 of the group so yes, there can be elements of the set such that $\alpha^k=1$. 11 is a prime number that does not divide the order of the group so, by Lagrange's theorem, it is impossible that $\alpha^{11}=1$. Finally, although 16 doesn't divide the order of the group and hence can't be the order

of any element in the group, there can elements of orders 2, 4 or 8 which, taken to the power 16, would give 1.

Remark: *the wording of the exam question was problematic because it did not exclude $\alpha = 1$, for which $\alpha^k = 1$ is always true for any k. One undergraduate and one graduate student noticed this and were given full points for the question.*

(iii) The orders must divide the order of the group so any number $2^{k_2} \times 2^{k_3} \times 5^{k_5} \times 7^{k_7}$ where $0 \le k_2 \le 3$, $0 \le k_3 \le 3$, $0 \le k_5 \le 1$ and $0 \le k_7 \le 1$, can be the order of elements in the multiplicative group, so there are $4 \times 4 \times 2 \times 2 = 64$ possible orders.

(g) (i) $X(1 + X^2) = X + X^3$ (since the degree is less than 4 there is no need to use any primitive polynomial or companion matrix in this operation)

(ii) Here we can use the companion matrix three times to evaluate $(1 + X^2)X^3$ as

$$[1010]\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}^3 = [0101]\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}^2 = [1110]\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix} = [0111]$$

yielding the result $X + X^2 + X^3$.

2. (a) $\beta = \alpha^3 = 8$ has order 4.

Remark: *$\beta = 5$ was also a valid answer. $\beta = 8$ is assumed throughout this crib, but all candidates using $\beta = 5$ consistently were marked as correct.*

(b)

$$F = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 8 & 12 & 5 \\ 1 & 12 & 1 & 12 \\ 1 & 5 & 12 & 8 \end{bmatrix} \quad F^{-1} = \frac{1}{4}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 5 & 12 & 8 \\ 1 & 12 & 1 & 12 \\ 1 & 8 & 12 & 5 \end{bmatrix} = \begin{bmatrix} 10 & 10 & 10 & 10 \\ 10 & 11 & 3 & 2 \\ 10 & 3 & 10 & 3 \\ 10 & 2 & 3 & 11 \end{bmatrix}$$

(c) Parity-check matrix is the first two rows of the DFT matrix, since the rate is $R = 1/2$,

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 8 & 12 & 5 \end{bmatrix}$$

(d) For frequency domain encoding, the encoder matrix consists of the last two rows of the inverse Fourier matrix, i.e.,

$$G = \begin{bmatrix} 10 & 3 & 10 & 3 \\ 10 & 2 & 3 & 11 \end{bmatrix}$$

Remark: *some candidates preferred to work with the systematic encoder matrix*

$$G = \begin{bmatrix} 1 & 0 & 8 & 4 \\ 0 & 1 & 7 & 5 \end{bmatrix}.$$

The question deliberately left the choice to the candidate and both solutions were counted as correct, as well as any equivalent encoder matrix for the same code.

(e) The code has $13^2 = 169$ codewords.

(f) The code can detect any pattern of at most 2 errors and correct any single error no matter where in a codeword it occurs.

(g) There is a transmission error because the received sequence is not a codeword, as can be verified by computing the syndrome

$$rH^T = [11, 12, 3, 4] \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 8 & 12 & 5 \end{bmatrix}^T = [4, 7]$$

which is clearly non-zero.

(h) Assuming a single error, the linear complexity of the error sequence is 1. Hence the full error sequence in the frequency domain is

$$[\alpha^2, \alpha^{11}, \alpha^8, \alpha^5] = [4, 7, 9, 6]$$

The full Fourier transform of the received sequence is

$$[11, 12, 3, 4] \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 8 & 12 & 5 \\ 1 & 12 & 1 & 12 \\ 1 & 5 & 12 & 8 \end{bmatrix} = [4, 7, 11, 9]$$

and hence we obtain the information sequence by substracting the relevant portion of the frequency domain error seqence

$$[11, 9] - [9, 6] = [2, 3].$$

Remark: *for those candidates using the systematic encoder matrix, decoding required a further step to compute the inverse DFT of* $[0, 0, 2, 3]$ *to yield* $[11, 12, 3, 0]$ *and hence the information sequence is* $[11, 12]$*. For those using other encoders, answers were verified by multiplying by the encoder matrix and verifying that the corresponding codeword is* $[11, 12, 3, 0]$*.*

3. (a) (i) A. The public key is $(m, e) = (143, 7)$ and hence the message $X = 42$ is encrypted as

$$Y = R_m(X^e) = R_{143}(42^7) = R_{143}(42 \times 42^2 \times 42^4) = R_{143}(42 \times 48 \times 16) = 81.$$

B. We note from the hint that $d = 120 - 17 = 103$ is the multiplicative inverse of 7 in $\mathbb{Z}_{\phi(m)} = \mathbb{Z}_{10\times12} = \mathbb{Z}_{120}$. Hence, the plaintext can be recovered from the ciphertext as

$$\begin{aligned} X = R_m(Y^d) &= R_{143}(81^{103}) = R_{143}(81 \times 81^2 \times 81^4 \times 81^{32} \times 81^{64}) \\ &= R_{143}(81 \times 126 \times 3 \times 126 \times 3) = 42. \end{aligned}$$

(ii) A. Exponentiation, e.g., X^n in a mulitplicative group, is the repeated application of the algebraic operation, i.e., "multiply X n times by itself". The equivalent in an additive group is to add a quantity n times, or in other words to multiply X by n. Hence, the equivalent of the Diffie-Hellman key protocol

in an additive group would require Alice to multiply an agreed basis α by a randomly chosen private key x_A modulo an agreed prime number p, and to publish the resulting public key $y_A = \alpha \cdot x_A \mod p$. Bob would do the same an publish $y_B = \alpha \cdot x_B \mod p$. Both could obtain a joint "secret" key by multiplying the other's public key by their secret key, i.e.,

$$s_{AB} = x_A y_B = \alpha x_A x_B = x_B y_A.$$

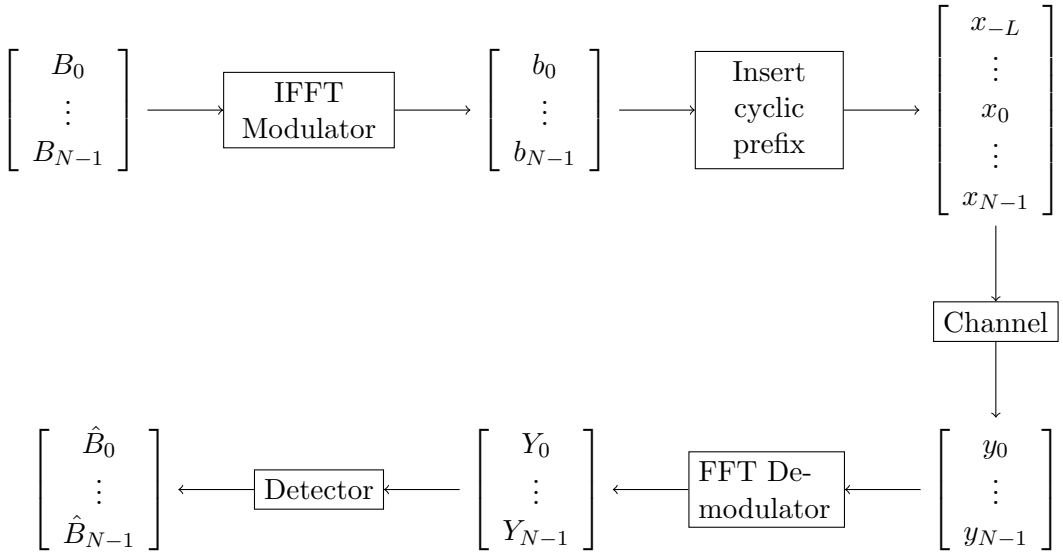
B. This is not secure because, unlike discrete exponentiation whose inverse the discrete logarithm is a reputedly computationally hard problem, the inverse of multiplication is not hard. The adversary can simply use Euclid's or Stein's extended gcd algorithm to determine the inverse α^{-1} of α modulo p, and then compute x_A and/or x_B from y_A and/or y_B, respectively, by multiplying the public keys by α^{-1} modulo p.

(b) (i) Let $B_0, \ldots, B_{N-1}$ represent the information symbols. We first generate the inverse FFT of $[B_0, \ldots, B_{N-1}]$ denoted by $[b_o, \ldots, b_{N-1}]$. We then append a cyclic prefix of length L, $[b_{N-L+1}, \ldots, b_{N-1}]$ to the start of $[b_o, \ldots, b_{N-1}]$ and transmit over the channel. The demodulator is an FFT computation which produces

$$Y_n = B_n H_n + W_n, \text{ for } n = 0, \ldots, N-1,$$

where H_n is the n-th DFT coefficient of the channel, i.e.,

$$H_n = \frac{1}{N} \sum_{k=0}^{N-1} h_k e^{-j\frac{2\pi}{N}kn}.$$



(ii) The minimum length of the cyclic prefix is L.

(iii) The role of the cyclic prefix is to eliminate Inter-Symbol Interference (ISI) between adjacent sub-carriers. To avoid ISI, we want the OFDM information symbols to be each multiplied by a single channel DFT coefficient. This is equivalent to cyclic convolution in the frequency domain. Since the channel actually acts

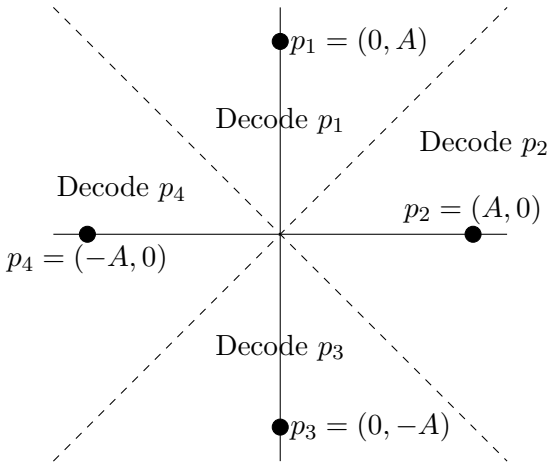
on the input via a linear rather than a cyclic convolution in the time domain, the cyclic prefix mimics a cyclic convolution by repeating the appropriate information at the beginning of the block.

4. (a) (i) The average energy per symbol is A^2. Therefore,

$$E_b = \frac{A^2}{2}$$

as each symbol corresponds to 2 bits.

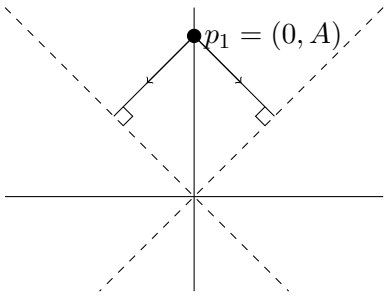
(ii) The decision regions are indicated by the dashed lines:



(iii) Since the symbols are equally likely and the constellation is symmetric, we can assume that symbol p_1 was transmitted, i.e.,

$$P_e = \Pr(\hat{X} \neq X | X = p_1).$$

Let N_1, N_2 be the two (orthogonal) components of N in the directions perpendicular to the decision boundaries, as shown in the figure below:



Since $N \sim \mathcal{CN}(0, N_0)$ is circularly symmetric complex Gaussian noise, N_1 and N_2 are independent and $\mathcal{N}(0, \frac{N_0}{2})$ (the components of N along any two orthogonal

directions will be independent and $\mathcal{N}(0, \frac{N_0}{2})$). Hence

$$P_e \leq \Pr\left(N_1 > \frac{\|p_2 - p_1\|}{2}\right) + \Pr\left(N_2 > \frac{\|p_4 - p_1\|}{2}\right) =$$
$$= \Pr\left(\frac{N_1}{\sqrt{\frac{N_0}{2}}} > \frac{A}{\sqrt{\frac{N_0}{2}}\sqrt{2}}\right) + \Pr\left(\frac{N_2}{\sqrt{\frac{N_0}{2}}} > \frac{A}{\sqrt{\frac{N_0}{2}}\sqrt{2}}\right)$$
$$= 2\,\mathrm{Q}\left(\frac{A}{\sqrt{N_0}}\right) = 2\,\mathrm{Q}\left(\sqrt{\frac{2E_b}{N_0}}\right).$$

(iv) The P_e for the AWGN channel, computed in Part 4(a)iii decays *exponentially* with $\frac{E_b}{N_0}$ because

$$2\,\mathrm{Q}\left(\sqrt{\frac{2E_b}{N_0}}\right) \leq e^{-E_b/N_0},$$

using $Q(x) \leq \frac{1}{2}e^{-x^2/2}$, for $x \geq 0$.

When there is fading, the effective SNR per bit is $|h|^2\frac{E_b}{N_0}$. Assuming Rayleigh fading, i.e., exponential distribution for $|h|^2$ and averaging over $|h|^2$, the expected probability of error will decay only *linearly* with $\frac{E_b}{N_0}$, i.e.,

$$P_e \approx \frac{C_1}{C_2 + \frac{E_b}{N_0}}$$

for some constants C_1 and C_2. This is because there is a non-negligible probability that the channel has a deep fade, i.e., $|h|^2 E_b \ll N_0$.

(b) The optimal decision rule is the MAP decision rule which reduces to the ML rule as the symbols $+1$ and -1 are equally likely,

$$\hat{x} = \arg\max_{x\in\{-1,+1\}} p(y_1, y_2|x).$$

We have

$$p(y_1, y_2|x) = p(N_1 = y_1 - x, N_2 = y_2 - N_1)$$
$$= p(N_1 = y_1 - x, N_2 = y_2 - y_1 + x).$$

Since N_1 and N_2 are independent and $\mathcal{N}(0, \sigma^2)$,

$$p(N_1 = y_1 - x, N_2 = y_2 - y_1 + x) = \frac{1}{2\pi\sigma^2} e^{-\frac{(y_1-x)^2}{2\sigma^2}} e^{-\frac{(y_2-y_1+x)^2}{2\sigma^2}}$$
$$= \frac{1}{2\pi\sigma^2} e^{\frac{-2(y_1-x)^2 - y_2^2 + 2(y_1-x)y_2}{2\sigma^2}}$$
$$= \frac{1}{2\pi\sigma^2} e^{\frac{1}{2\sigma^2}(-2y_1^2 - 2x^2 + 4y_1x - y_2^2 + 2y_1y_2 - 2xy_2)}.$$

Since $x^2 = 1$ and y_1 and y_2 are observed values, the decision rule is

$$\hat{x} = \arg\max_{x\in\{-1,+1\}} (4y_1x - 2y_2x)$$

which can be written as

$$\hat{x} = \arg\max_{x\in\{-1,+1\}} x(y_1 - \frac{y_2}{2}) = \begin{cases} 1, \text{ if } y_1 - \frac{y_2}{2} > 0, \text{ or} \\ -1 \text{ otherwise.} \end{cases}$$

Q1 Mathematical Fundamentals

29 attempts, Average mark 15.9/20, Maximum 20, Minimum 6.

This was an easy question composed of many small and largely independent parts that required calculations in number theory and finite fields. Only 1.f(ii) and (iii) were slightly tricky: in (ii) the vast majority of students said that there were no numbers that yielded 1 to the power 16, but this is wrong since any number that yields 1 to the power 8 yields $1^2=1$ to the power 16, which is not the same as having order 16. There was a slight omission in the question in that we should have specified that $\alpha \neq 1$, as $1^k=1$ for any k. This was noticed by two students who got full marks for the question as a result, and we have noted this in the exam crib for the benefit of future students during their revision. Surprisingly, only one student got 20/20 for the whole question, but the others did not consistently fail in the same parts, e.g., many students managed to answer the harder questions correctly but failed on small details in one or the other of the easier questions.

Q2 Reed Solomon Coding

35 attempts, Average mark 15.6/20, Maximum 20, Minimum 0.

The most popular question testing a coding and decoding technique that students had ample opportunity to play around with in one of the examples papers, in a manner that mirrored the example paper closely. Students did very well on this question in general, with many getting full marks. Those who struggled mostly took a valid but much harder way (e.g. working with the systematic encoder matrix rather than frequency domain encoding) and then made calculation errors. Counting codewords ($=q^k$) was also something many students struggled with. Many parts of the question simply tested knowledge and understanding of Reed-Solomon codes, e.g., when asked for the parity-check matrix students who knew that you could just cut the first rows of the DFT matrix got full points irrespective of whether they had got the DFT matrix right or wrong. The number of errors that can be detected was a misunderstood concept and will need to be taught more precisely next year.

Q3 Cryptography / OFDM

7 attempts, Average mark 12.9/20, Maximum 18, Minimum 4.

Very few students took this question, despite it being an easy question. The average is heavily weighed down by two exceptionally low marks, in one case of a student who did badly overall, and in the other case of a student who left this question for the end and ran out of time, not even attempting part (b) of the question. The average without these two would have been 15.8. The cryptography part of the question had one standard example of RSA mirroring a similar question in the examples paper, and one more challenging question on Diffie-Hellman that invited students to reflect on how the method would work in an addititive group. Only two students understood that the equivalent of exponentiation in an additive group is multiplication, and nobody made the link to the extended gcd algorithm that could be used to operate the inverse operation of multiplication and hence break the cipher efficiently. The OFDM part was book work and in the last part, anyone mentioning cyclic (or circular) convolution got full points, but there were still a few students who had not understood at all why we use a cyclic prefix in OFDM and hence did not make the link to cyclic convolution.

Q4 Wireless Communication

34 attempts, Average mark 14.0/20, Maximum 20, Minimum 3.

A very popular question that was selected by students probably because it appeared to be in line with many past questions, so a safe choice in an exam where the format had been modified to include a math question and half a cryptography question this year. However, the second part of the question was anything but trivial and this is reflected in the lower average mark for the question. Most students appeared to

understand the concepts well and those who failed in the first part did so on calculation errors or difficulty manipulating probability density functions. For the second part, a number of students tried manipulating random variables without writing the Maximum A-posterior Rules and thus got arbitrary results. The others either did well or failed on minor calculation errors but got partial points for this.

Jossy Sayir (Principal Assessor)