Topics in Discrete Mathematics: Introduction to Mathematical Cryptography. Solutions.

Dan Fretwell

Spring semester 2021/22

Chapter 1

1. (a) `QBT`.
   (b) `COW`.
   (c) You're on your own on this one...
   (d) The following four English words all Caesar shift to each other: `AX`, `BY`, `HE`, `IF`. My favourite example though is `YES` and `OUI` since they mean the same thing (in different languages).
2. (a) `FHOFGVGHGVBA`.
   (b) `CIPHER`.
   (c) You're on your own on this one...
3. (a) `XMVCYQHDP`.
   (b) `PICKLE RICK`.
   (c) You're on your own on this one...

Chapter 2

1. (a) The powers of $g = 2$ modulo 13 are $2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1$. This shows that g has order $12 = 13 - 1$ and so is a primitive root.
   (b) Suppose that $g^{\frac{p-1}{q}} = 1$ for some prime $q \mid p-1$. Then g has order less than $p-1$ and so is not a primitive root. Conversely, if the order k of g is less than $p-1$ then $k \mid \frac{p-1}{q}$ for some prime $q \mid p-1$. Then $g^{\frac{p-1}{q}} = (g^k)^{\frac{p-1}{qk}} = 1^{\frac{p-1}{qk}} = 1$. The claim follows by the contrapositive.
   (c) Since $29-1 = 28$ is only divisible by the primes 2 and 14 we need only check that $2^4, 2^{14} \not\equiv 1 \bmod 29$. This is simple since $2^4 \equiv \mathbf{16} \bmod 29$ and $2^{14} \equiv 2^4 \cdot (2^5)^2 \equiv 16 \cdot 9 \equiv 144 \equiv \mathbf{-1} \bmod 29$.

2. (a) Alice sends the following to Bob:

$$a = 2^{10} \equiv 3^2 \equiv \mathbf{9} \bmod 29.$$

Bob sends the following to Alice:

$$b = 2^{25} \equiv 3^5 \equiv (-2) \cdot 9 \equiv \mathbf{11} \bmod 29.$$

(b) Both compute shared key $s = 22$ since:

$$s_A = 11^{10} \equiv 5^5 \equiv 9 \cdot 25 \equiv -36 \equiv \mathbf{22} \bmod 29$$
$$s_B = 9^{25} \equiv 3^{50} \equiv 3^{-6} \equiv 10^6 \equiv 6 \cdot 5^6 \equiv 6 \cdot 9^2 \equiv 6 \cdot (-6) \equiv \mathbf{22} \bmod 29$$

3. Since $1 \leq k_A \leq \lfloor \log_g(p) \rfloor$ the integer g^{k_A} satisfies:

$$1 \leq g^{k_A} \leq g^{\lfloor \log_g(p) \rfloor} < g^{\log_g(p)} = p.$$

When Alice sends the value $a \equiv g^{k_A} \bmod p$ to Bob, no mod p reduction is taking place and she is actually sending the integer $a = g^{k_A}$.

If Eve intercepts this then she can then easily solve the corresponding Discrete Log Problem by using the standard log map (which is easy to compute, e.g. via Taylor expansion):

$$\mathrm{dlog}_g(a) = \log_g(g^{k_A}) + (p-1)\mathbb{Z} = k_A + (p-1)\mathbb{Z}.$$

From here she can intercept Bob's value $b = g^{k_B}$ and compute the shared key $s = b^{k_A} = g^{k_A k_B}$.

Chapter 3

1. (a) Let $N = p_1^{e_1} ... p_n^{e_n}$ for distinct primes p_i and let $P = \{p_1, ..., p_n\}$. We wish to count how many $1 \leq a \leq N$ are coprime with N. This is $N - b$ where b is the number of $1 \leq b \leq N$ that are divisible by at least one of the p_i.

The number of b divisible by one fixed prime $p_j \in P$ is $\frac{N}{p_j}$. The number of b divisible by two distinct primes $p_{j_1}, p_{j_2} \in P$ is $\frac{N}{p_1 p_2}$.

In general if $S \subseteq P$ then the number of b divisible by each prime $p \in S$ is $\frac{N}{\prod_{p \in S} p}$.

By Inclusion-Exclusion it follows that:

$$b = \sum_{1 \leq i \leq n} \frac{N}{p_i} - \sum_{1 \leq i < j \leq n} \frac{N}{p_i p_j} + \sum_{1 \leq i < j < k \leq n} \frac{N}{p_i p_j p_k} + ... + (-1)^{n-1} \frac{N}{p_1 p_2 ... p_n}.$$

It follows that

$$\begin{aligned} \phi(N) &= N \left(1 - \sum_{1 \leq i \leq n} \frac{1}{p_i} + \sum_{1 \leq i < j \leq n} \frac{1}{p_i p_j} - \sum_{1 \leq i < j < k \leq n} \frac{1}{p_i p_j p_k} + ... + (-1)^n \frac{1}{p_1 p_2 ... p_n} \right) \\ &= N \prod_{p | N} \left(1 - \frac{1}{p} \right). \end{aligned}$$

(b) $\phi(24) = 24\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) = 8$, $\phi(25) = 25\left(1-\frac{1}{5}\right) = 20$, $\phi(26) = 26\left(1-\frac{1}{2}\right)\left(1-\frac{1}{13}\right) = 12$.

2. (a) Bob's public key is $(11, 85)$ and his private key is $d = 35$, since $d \equiv 11^{-1} \equiv \mathbf{35} \bmod 64$ (use Euclid's algorithm or notice that $6 \cdot 64 + 1 = 385 = 11 \cdot 35$).

   (b) Alice sends $c = 64$ since:

$$c = f_{11}(4) = 4^{11} \equiv (4^4)^3 \cdot 4^{-1} \equiv 4^{-1} \equiv -21 \equiv \mathbf{64} \bmod 85.$$

   (The answer being 64 and $\phi(N) = 64$ is a coincidence!).

   (c) Bob decrypts by calculating:

$$m = f_{35}(64) = 64^{35} \equiv 4^{105} \equiv 4 \cdot (4^4)^{26} \equiv \mathbf{4} \bmod 85.$$

3. The encrypted message that Eve sends is $c \equiv m^e \bmod N$. However the integer m^e satisfies:

$$1 \leq m^e < (N^{\frac{1}{e}})^e = N,$$

   and so no mod N reduction is done when computing c. Thus $c = m^e$ and Eve can simply take the e-th root of c to recover m.

4. (a) This number is even and so $2 \mid N$ (the other factor is prime).

   (b) The digit sum of this number is $66 \equiv 0 \bmod 3$ and so $3 \mid N$ (the other factor is prime).

   (c) The last digit is 5 and so $5 \mid N$ (the other factor is prime).

Chapter 4

1. (a) We need to solve the congruence $4x \equiv 13 \bmod 45$. this has solution $x \equiv 13 \cdot 4^{-1} \equiv 13 \cdot (-11) \equiv -143 \equiv \mathbf{37} \bmod 45$. Thus $\mathrm{dlog}_4(13) = 37 + 45\mathbb{Z}$.

   (b) The consecutive powers of 5 mod 23 are $5, 2, 10, 4, 20, 8, 17, 16, \ldots$ and so $\mathrm{dlog}_5(16) = 8 + 22\mathbb{Z}$.

   (c) Direct computation gives $A^3 = B$ and since $B^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ we have that the order of B divides 6. One can check that it equals 6 since $A^2 \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Thus $\mathrm{dlog}_A(B) = 3 + 6\mathbb{Z}$.

2. (a) Alice computes:

$$c_1 = 2^3 \equiv \mathbf{8} \bmod 13$$
$$c_2 = 9 \cdot 6^3 \equiv (-4 \cdot 6) \cdot 6^2 \equiv 2 \cdot (-3) \equiv \mathbf{7} \bmod 13.$$

   (b) Bob computes:

$$m = c_2 c_1^{-5} = 7 \cdot 8^{-5} \equiv 7 \cdot 5^5 \equiv 7 \cdot 5 \cdot (-1)^2 \equiv 35 \equiv \mathbf{9} \bmod 13.$$

(c) Since $s = 3 < \log_2(13)$ (normal log) no reduction took place when working out c_1 (i.e. we just got $2^3 = 8$). Hence Eve can simply find Alice's secret value by calculating $s = \log_2(8) = 3$ (normal log). From here she can calculate h^s and work out m by calculating $m = c_2 h^{-s}$.

Chapter 5

1. (a) Alice sends $(14, 20)$, since $m_0 = 14$ and:

$$m_1 = f_7(14) = 14^7 \equiv 14 \cdot (-2)^3 \equiv -14 \cdot 8 \equiv \mathbf{20} \bmod 33.$$

   (b) Bob verifies the message by calculating

$$f_3(20) = 20^3 \equiv -13^3 \equiv -13 \cdot 4 \equiv \mathbf{14} \bmod 33$$

   and noting that this equals m_0.

2. (a) Alice sends $(7, 14, 9)$, since $m_0 = 7$ and:

$$\begin{aligned} m_1 &= 3^9 \equiv 10^3 \equiv 10 \cdot 15 \equiv 10 \cdot (-2) \equiv \mathbf{14} \bmod 17 \\ m_2 &= (7 - 5 \cdot 14)9^{-1} \equiv 9^{-1} \equiv \mathbf{9} \bmod 16 \end{aligned}$$

   (b) Bob verifies the message by calculating

$$\begin{aligned} g^{m_0} &= 3^7 \equiv 3 \cdot 10^2 \equiv 3 \cdot 15 \equiv \mathbf{11} \bmod 17 \\ h^{m_1} m_1^{m_2} &= 5^{14} \cdot 14^9 \equiv 5^5 \cdot 70^9 \equiv 5^5 \cdot 2^9 \equiv 10^5 \cdot 16 \\ &\equiv 15^2 \cdot 10 \cdot 16 \equiv 4 \cdot 7 \equiv \mathbf{11} \bmod 17 \end{aligned}$$

   and noting that they are equal.

3. Suppose the two signatures are (m_0, m_1, m_2) and (m_0', m_1', m_2'). Since the same public/private key and secret value has been used it follows that $m_1 = g^s = m_1'$. Eve would notice this instantly.

   It would also follow that

$$\begin{aligned} m_2 &\equiv (m_0 - k m_1) s^{-1} \bmod p - 1 \\ m_2' &\equiv (m_0' - k m_1) s^{-1} \bmod p - 1. \end{aligned}$$

   Eliminating s and rearranging gives:

$$k \equiv (m_0' - m_0 m_2' m_2^{-1})(m_1' - m_1 m_2' m_2^{-1})^{-1} \bmod p - 1.$$

   This is something that Eve can compute given knowledge of the two signatures.

Chapter 6

1. (a) Yes, $111 = 3 + 27 + 81$.
   (b) No, $27 = 1 + 5 + 7 + 14$.
   (c) Yes, $245 = 10 + 24 + 211$.
   (d) No, $461 = 114 + 129 + 101 + 117$.

2. The nth term of the sequence is $x_m = 2^{m-1}a - (2^{m-1} - 1)b$ and the nth term of the partial sum sequence is $y_m = (2^m - 1)a - (2^m - (m + 1))b$. Consider the difference:

   $$x_{m+1} - y_m = (2^m a - (2^m - 1)b) - ((2^m - 1)a - (2^m - (m+1))b) = a - bm.$$

   This is positive for all $1 \leq m \leq n$ since $a > bn$, and so x_n is a superincreasing sequence of length n. (Note that when $b = 0$ this sequence is superincreasing for all lengths).

3. (a) Bob's public key is the sequence $53, 39, 64, 22, 30, 99$.
   (b) Alice sends $c = 39 + 64 + 99 = 202$.
   (c) Bob computes $53^{-1} \cdot 202 \equiv 77 \cdot 82 \equiv \mathbf{74} \bmod 120$. Solving the corresponding superincreasing Knapsack Problem gives the required bit string $\mathbf{x} = 011001$.

Chapter 7

1. Using Lagrange Interpolation:

$$\begin{aligned} f(x) &= 4\frac{(x-2)(x-3)(x-4)}{(1-2)(1-3)(1-4)} + 9\frac{(x-1)(x-3)(x-4)}{(2-1)(2-3)(2-4)} \\ &\quad + 1\frac{(x-1)(x-2)(x-4)}{(3-1)(3-2)(3-4)} + 3\frac{(x-1)(x-2)(x-3)}{(4-1)(4-2)(4-3)} \\ &= -\frac{2}{3}(x-2)(x-3)(x-4) + \frac{9}{2}(x-1)(x-3)(x-4) \\ &\quad - \frac{1}{2}(x-1)(x-2)(x-4) + \frac{1}{2}(x-1)(x-2)(x-3) \\ &= \frac{23}{6}x^3 - \frac{59}{2}x^2 + \frac{200}{3}x - 37 \end{aligned}$$

2. (a) Alice distributes the points $P_1 = (1, 1), P_2 = (2, 11), P_3 = (3, 11), P_4 = (4, 7), P_5 = (5, 5), P_6 = (6, 11)$.
   (b) For example, suppose the first four employees get together. Applying

Lagrange Interpolation to P_1, P_2, P_3, P_4 gives:

$$\begin{aligned} f(x) &= \frac{(x-2)(x-3)(x-4)}{(1-2)(1-3)(1-4)} + 11\frac{(x-1)(x-3)(x-4)}{(2-1)(2-3)(2-4)} \\ &\quad + 11\frac{(x-1)(x-2)(x-4)}{(3-1)(3-2)(3-4)} + 7\frac{(x-1)(x-2)(x-3)}{(4-1)(4-2)(4-3)} \\ &= 14(x-2)(x-3)(x-4) + 14(x-1)(x-3)(x-4) \\ &\quad + 3(x-1)(x-2)(x-4) + 4(x-1)(x-2)(x-3) \\ &= \mathbf{9} + 2x + 6x^2 + x^3. \end{aligned}$$

The constant term agrees with the secret $S = 9$.