An Introduction to Mathematical Cryptography
Notes and Exercises

John Peloquin

Chapter 1

Exercise (1.5)**.** Suppose A is an alphabet of n letters.

(a) There are $n!$ simple substitution ciphers on A.

(b) Define the function $!n$ recursively by[1]

$$!n = \begin{cases} 1 & \text{if } n = 0 \\ 0 & \text{if } n = 1 \\ n! - \sum_{k=1}^{n} \binom{n}{k} \cdot !(n-k) & \text{if } n > 1 \end{cases}$$

(i) There are $!n$ simple substitution ciphers on A leaving no letters fixed.

(ii) There are $n! - !n$ simple substitution ciphers on A leaving at least one letter fixed.

(iii) There are $n \cdot !(n-1)$ simple substitution ciphers on A leaving exactly one letter fixed.

(iv) There are $n! - !n - n \cdot !(n-1)$ simple substitution chipers on A leaving at least two letters fixed.

Proof. For (a), note that a simple substitution cipher on A is just a permutation of A, and there are $n!$ permutations of A.

For (b), we prove (i) by induction on n. Cases $n = 0, 1$ are trivial. Suppose $n > 1$ and the result is true for all $m < n$. Let φ_k be the number of permutations

[1] A more efficient recursive definition for $n > 1$ is given by $!n = (n-1)[!(n-1) + !(n-2)]$.

of A fixing exactly k elements, for $1 \le k \le n$. Clearly the desired number is

$$n! - \sum_{k=1}^{n} \varphi_k$$

To compute φ_k, note that in order to permute the elements of A while fixing k elements, we must choose k elements to fix and then permute the remaining $n-k$ elements without fixing any of them. The number of possible ways to choose k elements from A is just $\binom{n}{k}$. By induction, the number of ways to permute the remaining $n-k$ elements without fixing any of them is $!(n-k)$. So $\varphi_k = \binom{n}{k} \cdot !(n-k)$.

Now (ii) follows trivially from (a) and (i); (iii) follows from the proof of (ii) by taking φ_1; and (iv) follows trivially from (a), (i), and (iii). □

For example, when $n = 4$, there are 24 simple substitution ciphers, 9 of which leave no letters fixed, 15 of which leave at least one letter fixed, 8 of which leave exactly one letter fixed, and 7 of which leave at least two letters fixed.

Exercise (1.11)**.** Let a and b be positive integers.

(a) If u and v are integers with $au + bv = 1$, then $\gcd(a, b) = 1$.

(b) If u and v are integers with $au + bv = 6$, it is not necessarily true that $\gcd(a, b) = 6$, but $\gcd(a, b)$ will be a divisor of 6.

(c) If (u_1, v_1) and (u_2, v_2) are solutions of $au + bv = 1$, then a divides $v_2 - v_1$ and b divides $u_2 - u_1$.

(d) If $g = \gcd(a, b)$ and (u_0, v_0) is a solution to $au + bv = g$, then each other solution has the form

$$u = u_0 + \frac{kb}{g} \qquad v = v_0 - \frac{ka}{g}$$

for some integer k.

Proof. (a) Trivially $1 \mid a$ and $1 \mid b$. If $d \mid a$ and $d \mid b$, then $d \mid au$ and $d \mid bv$, so $d \mid au + bv = 1$.

(b) Let $a = b = 3$ and $u = v = 1$. Then $au + bv = 6 \neq 3 = \gcd(a, b)$. The second claim follows from the proof of (a).

(c) We have

$$\begin{aligned}au_1 + bv_1 &= au_2 + bv_2\\ au_1 - au_2 &= bv_2 - bv_1\\ a(u_1 - u_2) &= b(v_2 - v_1)\end{aligned}$$

Now $a \mid b(v_2 - v_1)$, but $\gcd(a, b) = 1$ by (a), so $a \mid v_2 - v_1$. Similarly $b \mid u_2 - u_1$.

(d) If (u, v) is another solution, then

$$au_0 + bv_0 = au + bv = g$$

Dividing by g, this becomes

$$\frac{a}{g}u_0 + \frac{b}{g}v_0 = \frac{a}{g}u + \frac{b}{g}v = 1$$

Let $a' = a/g$ and $b' = b/g$. By the proof of (c), there exists k such that $ka' = v_0 - v$ and $kb' = u - u_0$, so

$$u = u_0 + kb' = u_0 + \frac{kb}{g} \qquad v = v_0 - ka' = v_0 - \frac{ka}{g} \qquad \square$$

Exercise (1.21)**.** Let $m > 1$.

(a) If m is odd, then $(m+1)/2 = 2^{-1} \bmod m$.

(b) If $b > 0$ and $m \equiv 1 \bmod b$, then

$$\frac{(b-1)(m-1)}{b} + 1 = b^{-1} \bmod m$$

Proof. Note (a) follows from (b) by taking $b = 2$, so it is sufficient to prove (b).

Since $b \mid m-1$, the quantity on the left of the equation is an integer, and since $m > 1$,

$$\begin{aligned}0 &\le (b-1)(m-1) < b(m-1)\\ 0 &\le \frac{(b-1)(m-1)}{b} < m-1\\ 1 &\le \frac{(b-1)(m-1)}{b} + 1 \le m-1\end{aligned}$$

Finally,

$$b\left[\frac{(b-1)(m-1)}{b} + 1\right] = (b-1)(m-1) + b = (b-1)m + 1 \equiv 1 \bmod m \qquad \square$$

Exercise (1.26)**.** There are infinitely many primes.

Proof. Suppose there are only finitely many primes, say $p_1, \ldots, p_k$. Let

$$N = p_1 \cdots p_k + 1$$

By the fundamental theorem of arithmetic, there exists a prime p with $p \mid N$, so $N \equiv 0 \bmod p$. But by assumption, $p = p_i$ for some $1 \le i \le k$, so $p \mid p_1 \cdots p_k$ and hence $N \equiv 1 \bmod p$, a contradiction. $\square$

Exercise (1.33)**.** If p is prime, $q = (p-1)/2$ is also prime, $0 < g < p$, $g \not\equiv \pm 1 \bmod p$, and $g^q \not\equiv 1 \bmod p$, then g is a primitive root mod p.

Proof. Let n be the order of g mod p. We claim $n = p - 1$.

By assumption, $g^q \not\equiv 1 \bmod p$, but by Fermat's little theorem,

$$(g^q)^2 = g^{2q} = g^{p-1} \equiv 1 \bmod p$$

Therefore g^q has order 2 mod p, and hence $2 \mid n$ by Lagrange's theorem. If $n = 2$, then $g^2 \equiv 1 \bmod p$, hence $g \equiv \pm 1 \bmod p$, contrary to our assumption. So we must have $n > 2$.

Now $n \mid p - 1$, so $p - 1 = nk = 2jk$ for some integers j and k with $j > 1$. But since $jk = (p-1)/2 = q$ is prime, this means $k = 1$ and hence $n = p - 1$ as desired. $\square$

Exercise (1.46)**.** The XOR cipher defined on bit strings by

$$e_k(m) = k \oplus m \qquad \text{and} \qquad d_k(c) = k \oplus c$$

is not secure against a chosen plaintext attack.

Proof. If the pair m and $c = k \oplus m$ are known, then k is easily recovered as

$$c \oplus m = (k \oplus m) \oplus m = k \oplus (m \oplus m) = k \oplus 0 = k \qquad \square$$

For example, working with 16-bit strings, if $m = 0010010000101100$ and $c = 1001010001010111$, then $k = 1011000001111011$.

Chapter 2

Exercise (2.3)**.** Let g be a primitive root modulo p. Define

$$\log_g : \mathbb{F}_p^* \to \mathbb{Z}/(p-1)\mathbb{Z}$$

as follows: for $h \in \mathbb{F}_p^*$, $\log_g(h) = x$ if and only if $0 \leq x < p-1$ and $g^x = h$. Then $\log_g$ witnesses an isomorphism from $\mathbb{F}_p^*$ to $\mathbb{Z}/(p-1)\mathbb{Z}$.

Proof. First observe that $\log_g$ is well defined. Since g is a primitive root mod p, for each $h \in \mathbb{F}_p^*$ there exists at least one $0 \leq x < p-1$ such that $g^x = h$. If $0 \leq x, y < p-1$ and $g^x = h = g^y$, then $g^{x-y} = 1$, so $p-1 \mid x-y$ and hence $x = y$.

Observe also that $\log_g$ is injective. If $h_1, h_2 \in \mathbb{F}_p^*$ and $\log_g h_1 = x = \log_g h_2$, then $h_1 = g^x = h_2$. Since $\mathbb{F}_p^*$ and $\mathbb{Z}/(p-1)\mathbb{Z}$ both have order $p-1$, this this also shows that $\log_g$ is surjective, and hence bijective.

If $h_1, h_2 \in \mathbb{F}_p^*$, we claim that

$$\log_g(h_1 h_2) \equiv \log_g h_1 + \log_g h_2 \pmod{p-1}$$

Indeed, let $x_1 = \log_g h_1$ and $x_2 = \log_g h_2$, so $h_1 = g^{x_1}$ and $h_2 = g^{x_2}$. Then $h_1 h_2 = g^{x_1} g^{x_2} = g^{x_1+x_2}$, so $\log_g(h_1 h_2) \equiv x_1 + x_2 \bmod p-1$ as claimed. This shows that $\log_g$ is a homomorphism, and since it is bijective, an isomorphism. □

Note by induction and the fact that $\log_g(h^{-1}) \equiv -\log_g(h) \bmod p-1$ for all $h \in \mathbb{F}_p^*$, it also follows that

$$\log_g(h^n) \equiv n \log_g h \pmod{p-1}$$

for all $h \in \mathbb{F}_p^*$ and $n \in \mathbb{Z}$.

Exercise (2.4)**.** Using the brute force algorithm of computing powers $g^x \bmod p$ manually for $x = 0, 1, 2, \ldots$ we obtain the following discrete logarithms:

(a) $\log_2 13 = 7 \bmod 23$

(b) $\log_{10} 22 = 11 \bmod 47$

(c) $\log_{627} 608 = 18 \bmod 941$

Exercise (2.5)**.** Let p be an odd prime and g be a primitive root modulo p. Then a has a square root modulo p if and only if $\log_g a$ is even.

Proof. Since $\log_g$ is a homomorphism (Exercise 2.3), we know that

$$\log_g(x^2) \equiv 2\log_g(x) \pmod{p-1}$$

for all $x \in \mathbb{F}_p^*$, from which the desired result follows immediately. $\square$

Exercise (2.9)**.** A Diffie-Hellman oracle can be used to decrypt arbitrary ElGamal ciphertexts.

Proof. Let p and g be known parameters for ElGamal encryption. Given an ElGamal ciphertext (c_1, c_2), we know that $c_1 = g^k \bmod p$ for some ephemeral key k and $c_2 = mA^k = m(g^a)^k = mg^{ak} \bmod p$ for some plaintext message m and public key $A = g^a \bmod p$ with corresponding private key a. Now given $A = g^a$ and $c_2 = g^k$, a Diffie-Hellman oracle provides us with g^{ak}, with which we can easily compute $m = c_2(g^{ak})^{-1}$. $\square$

This result shows that decrypting arbitrary ElGamal ciphertexts is no harder than the Diffie-Hellan problem. Together with the converse result (Proposition 2.10), this result shows that the difficulty of decrypting arbitrary ElGamal ciphertexts is equal to that of the Diffie-Hellman problem.

Exercise (2.17)**.** Using the Shanks algorithm, we obtain the following discrete logarithms:

(a) $\log_{11} 21 = 37 \bmod 71$

First we compute $n = \lfloor\sqrt{71}\rfloor + 1 = 8 + 1 = 9$. For $i = 0, \ldots, 9$ we compute values $11^i \bmod 71$ to obtain the following list:

i	0	1	2	3	4	5	6	7	8	9
$11^i \bmod 71$	1	11	50	53	15	23	40	14	12	61

Now we compute $u = 11^{-n} = 11^{-9} = (11^9)^{-1} = 61^{-1} = 7 \bmod 71$. For $j = 0, \ldots, 9$ we compute values $21 \cdot 7^j \bmod 71$ until we find a match:

j	0	1	2	3	4
$21 \cdot 7^j \bmod 71$	21	5	35	32	11

We find a match 11 at $i = 1$ and $j = 4$, so $x = i + jn = 1 + 4 \cdot 9 = 37$ is the logarithm. Indeed, $11^{37} \equiv 21 \bmod 71$.

Exercise (2.18)**.** Using the Chinese remainder algorithm, we obtain solutions to the following systems of congruences:

(a) $x \equiv 3 \bmod 7$ and $x \equiv 4 \bmod 9$.

We start with the solution $x = 3$ to the first congruence. To find a solution to both congruences, we must find a solution to the second congruence which lies in the solution space of the first, which is $x + 7y$ for $y \in \mathbb{Z}$. Such a solution must satisfy

$$\begin{aligned} 3 + 7y &\equiv 4 \pmod 9 \\ 7y &\equiv 1 \pmod 9 \\ y &\equiv 4 \pmod 9 && \text{since } 7^{-1} \equiv 4 \bmod 9 \end{aligned}$$

We take $y = 4$ to yield the solution $3 + 7 \cdot 4 = 31$. Indeed, $31 \equiv 3 \bmod 7$ and $31 \equiv 4 \bmod 9$ as desired.

(d) $x \equiv 5 \bmod 9$ and $x \equiv 6 \bmod 10$ and $x \equiv 7 \bmod 11$.

We start with the solution $x = 5$ to the first congruence. Proceeding as in (a), we obtain a solution to the first and second congruences by solving

$$\begin{aligned} 5 + 9y &\equiv 6 \pmod{10} \\ 9y &\equiv 1 \pmod{10} \\ y &\equiv 9 \pmod{10} && \text{since } 9^{-1} \equiv 9 \bmod 10 \end{aligned}$$

We take $y = 9$ to yield the solution $5 + 9 \cdot 9 = 86$. Indeed, $86 \equiv 5 \bmod 9$ and $86 \equiv 6 \bmod 10$ as desired.

To find a solution to all three congruences, we must find a solution to the third congruence which lies in the *intersection* of the solution spaces of the first two, which is $86 + 9 \cdot 10z$ for $y \in \mathbb{Z}$. Such a solution must satisfy

$$\begin{aligned} 86 + 90z &\equiv 7 \pmod{11} \\ 9 + 2z &\equiv 7 \pmod{11} \\ 2z &\equiv 9 \pmod{11} \\ z &\equiv 10 \pmod{11} && \text{since } 2^{-1} \equiv 6 \bmod 11 \end{aligned}$$

We take $z = 10$ to yield the solution $86 + 90 \cdot 10 = 986$. Indeed, $986 \equiv 5 \bmod 9$, $986 \equiv 6 \bmod 10$, and $986 \equiv 7 \bmod 11$.

Exercise (2.25)**.** Let p and q be distinct odd primes and let $n = pq$.

(a) If $\gcd(a, n) = 1$ and a has a square root modulo n, then a has four square roots modulo n.

Proof. (a) Let r be a square root of a modulo n. Then x is a square root of a modulo n if and only if $x^2 \equiv a \equiv r^2 \bmod n$, which is true if and only if $x^2 \equiv r^2 \bmod p$ and $x^2 \equiv r^2 \bmod q$, which is true if and only if $x \equiv \pm r \bmod p$ and $x \equiv \pm r \bmod q$, since p and q are distinct primes.

This implies that the square roots of a modulo n are just the solutions to the following systems of congruences:

$$
\begin{aligned}
x &\equiv r \pmod{p} && \text{and} && x \equiv r \pmod{q} && (1)\\
x &\equiv r \pmod{p} && \text{and} && x \equiv -r \pmod{q} && (2)\\
x &\equiv -r \pmod{p} && \text{and} && x \equiv r \pmod{q} && (3)\\
x &\equiv -r \pmod{p} && \text{and} && x \equiv -r \pmod{q} && (4)
\end{aligned}
$$

Since $p \neq q$, the Chinese remainder theorem guarantees that for each one of these systems, there is a unique solution modulo $n = pq$. This implies that there are *at most* four square roots of a modulo n.

Now r is one of the roots, and clearly so is $-r$. Note r is also a unit since a is a unit (because $\gcd(a, n) = 1$). If $r \equiv -r \bmod n$, then $1 \equiv -1 \bmod n$, so $2 \equiv 0 \bmod n$—a contradiction since $n > 2$. Therefore r and $-r$ are distinct. Note r satisfies the first system, and $-r$ satisfies the last system. Let s be the solution to the second system. Then $-s$ is the solution to the third system, and s and $-s$ are also distinct. If $r \equiv s \bmod n$, then $r \equiv -r \bmod q$, so $2 \equiv 0 \bmod q$—a contradiction since $q > 2$. Therefore r and s are distinct. Similarly r and $-s$ are distinct since $p > 2$. Therefore $\{\pm r, \pm s\}$ are the four square roots of a modulo n. □

References

[1] Hoffstein, J. and J. Pipher and J. H. Silverman. *An Introduction to Mathematical Cryptography.* Springer, 2008.