The University of Sydney
School of Mathematics and Statistics

Tutorial 8 (Week 10)

MATH2068/2988: Number Theory and Cryptography — Semester 2, 2017

Web Page: http://www.maths.usyd.edu.au/u/UG/IM/MATH2068/
Lecturer: Dzmitry Badziahin

More difficult questions are marked with either * or **. Those marked * are at the level which MATH2068 students will have to solve in order to be sure of getting a Credit, or to have a chance of a Distinction or High Distinction. Those marked ** are mainly intended for MATH2988 students.

In the Diffie–Hellman key exchange protocol, Alice posts a public key (p, b, k) where p is a prime, b is a nonzero residue mod p, and k is the residue of b^x mod p for some nonnegative integer x, which is Alice's private key. Bob responds with c, the residue of b^y mod p where y is a nonnegative integer which is Bob's private key. Then Alice and Bob have a shared secret number s, the residue of b^{xy} mod p, since $s \equiv k^y \equiv c^x \pmod{p}$.

In the Elgamal cryptosystem, s is used as a scrambling factor to multiply residues mod p. After Alice has posted her public key (p, b, k), Bob chooses a private key y, computes the residue c of b^y mod p, and also computes the shared secret s as the residue of k^y mod p. Having encoded his message as a residue M mod p (or, for a longer message, a sequence $[M_1, \cdots, M_\ell]$ of such residues), he encrypts it by replacing M with the residue M' of sM mod p (or by replacing each M_i with the residue M'_i of sM_i mod p). The ciphertext he sends is $\langle c, M' \rangle$ (or $\langle c, [M'_1, \cdots, M'_\ell] \rangle$). Alice can compute s as the residue of c^x mod p, and can thus decrypt the message by multiplying by the inverse of s.

Tutorial Exercises:

1. This question illustrates the Diffie–Hellman key exchange protocol with small (and hence unrealistic) numbers. Suppose that Alice posts the public key $(31, 3, 13)$.

(a) If you are Bob, and choose your private key to be 4, what should you send to Alice, and what is the shared secret number that results?

(b) Solve $3^x \equiv 13 \pmod{31}$ to find Alice's private key.

(c) Now suppose you are an eavesdropper who has worked out Alice's private key as in the previous part. If you overhear that Bob's message to Alice is 5, what is their shared (supposedly) secret number?

2. Amy, a user of the Elgamal cryptosystem, has posted the public key $(47, 5, 2)$.

(a) Encrypt the message $[12, 26, 33]$ to send to Amy, choosing 7 as your private key.

(b) Now suppose you are an eavesdropper who wants to decrypt messages sent to Amy. You calculate that $5^{18} \equiv 2 \pmod{47}$, which means that 18 is Amy's private key. Use this knowledge to decrypt the ciphertext $\langle 8, [17, 29, 35] \rangle$.

3. Let p be a prime and $b \in \{1, \cdots, p-1\}$ a primitive root modulo p; recall that this means that $\mathrm{ord}_p(b) = p-1$. For any $a \in \{1, \cdots, p-1\}$, there is a unique $i \in \{0, 1, \cdots, p-2\}$ such that $b^i \equiv a \pmod{p}$; we call this i the discrete logarithm of a to the base b modulo p, written $\log_{b,p}(a)$. This exercise shows that some of the usual logarithm laws hold for discrete logarithms, if interpreted appropriately.

(a) Suppose $a_1, a_2, a_3 \in \{1, \cdots, p-1\}$ satisfy $a_3 \equiv a_1 a_2 \pmod{p}$. Show that

$$\log_{b,p}(a_3) \equiv \log_{b,p}(a_1) + \log_{b,p}(a_2) \pmod{p-1}.$$

(b) Suppose $a_1, a_2 \in \{1, \cdots, p-1\}$ are inverse to each other mod p. Show that

$$\log_{b,p}(a_2) \equiv -\log_{b,p}(a_1) \pmod{p-1}.$$

(c) Suppose $b' \in \{1, \cdots, p-1\}$ is another primitive root modulo p. Show that for any $a \in \{1, \cdots, p-1\}$ we have

$$\log_{b,p}(a) \equiv \log_{b,p}(b') \log_{b',p}(a) \pmod{p-1}.$$

4. Show that 3 is a primitive root modulo 19, and make a table giving the values of $\log_{3,19}(a)$ for all nonzero residues a modulo 19. Which other nonzero residues are primitive roots?

5. If m is any positive integer and $b \in \mathbb{Z}$, we say that b is a primitive root modulo m if $\gcd(b, m) = 1$ and $\mathrm{ord}_m(b) = \phi(m)$. It was proved in lectures that such primitive roots always exist when m is prime; this question investigates the case where $m = p^k$ for p a prime and $k \geq 2$.

*(a) It is easy to see that 3 is a primitive root modulo 4. However, there is no primitive root modulo 8, because 3, 5, and 7 all have order 2 modulo 8. Deduce that there is no primitive root modulo 2^k where $k \geq 4$.

**(b) Show that if $m = p^k$ where p is an odd prime and $k \geq 2$, then there is a primitive root modulo m. (Hint: show that there is a primitive root b modulo p which satisfies $b^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$ for all $k \geq 2$.)

Extra Exercises:

6. Your Elgamal public key is $(3937201, 158, 7111)$, your private key being 3. You receive the ciphertext $\langle 61320, 62799 \rangle$. Decrypt it to find the original message.

***7.** Suppose that m has prime factorization $p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ where $p_1, p_2, \cdots, p_r$ are distinct primes and $k_1, k_2, \cdots, k_r \in \mathbb{Z}^+$. Let $b \in \mathbb{Z}$ be such that $\gcd(b, m) = 1$.

(a) Show that $\mathrm{ord}_m(b)$ is the least common multiple of $\mathrm{ord}_{p_1^{k_1}}(b), \cdots, \mathrm{ord}_{p_r^{k_r}}(b)$.

(b) Hence show that b is a primitive root modulo m if and only if the following two conditions hold: (i) b is a primitive root modulo $p_i^{k_i}$ for all $i \in \{1, \cdots, r\}$, and (ii) the numbers $\phi(p_1^{k_1}), \cdots, \phi(p_r^{k_r})$ are pairwise coprime.

(c) Combine this with Q5 to determine which moduli m have primitive roots.

Selected numerical answers:

1. (a) 19, 10 (b) 11 (c) 25 **2.** (a) $\langle 11, [32, 38, 41] \rangle$ (b) $[12, 26, 33]$