Cryptology - Week 2 worksheet

These exercises are to aid your learning on the lecture material from week 2. If necessary also supported by the extra notes on modular arithmetic (now including the Chinese Remainder Theorem).

- Question 1 is some practise with modular arithmetic (including inversion).
- Question 2 is about the Diffie-Hellman key exchange.
- Question 3 is about ElGamal encryption.
- Questions 4 and 5 are developping some mathematical tools to encrypt a message using RSA.
- Question 6 is about RSA.

1. For each calculation, where possible please give your answer as $a \pmod{n}$ where $0 \leq a < n$.
   (a) Compute $5 + 8 \pmod{10}$.
   (b) Compute $8 - 19 \pmod{23}$.
   (c) Compute $13 \times 16 \pmod{25}$.
   (d) Compute the inverse of $6 \pmod{11}$, if it exists.
   (e) Compute the inverse of $6 \pmod{9}$, if it exists.
   (f) Which $a \pmod{5}$ have an inverse?
   (g) Which $a \pmod{6}$ have an inverse?

2. (a) Using the public parameters $(p, g) = (37, 2)$, Hellman sends you his public key $g^h = 5$. Your secret key is $d = 6$. Compute your shared secret with Hellman.
   (b) Prove that Hellman's secret $\mathrm{sk_H} = h$ is only defined mod 36, i.e., that you could imitate Hellman using any secret key of the form $\mathrm{sk_H} + 36n$, for $n \in \mathbb{Z}$.
   (c) Using the Chinese Remainder Theorem to compute discrete logarithms (h^{th} roots mod 36), compute Hellman's secret (mod 36).

3. (a) Hellman contacts you to tell you that he wants to send you an encrypted message. You choose parameters $p = 37$, $g = 2$, and $sk = d = 7$, compute $pk = 2^7 \pmod{37} = 17$, and send Hellman $(p, g, pk) = (37, 2, 17)$. Hellman replies with the ciphertext

$$(pk_H, enc_m) = (9, 13).$$

Decrypt the message. (Note: the 'message' is just a number mod 37).

(b) You ask Hellman to share the message with Alice. You observe Hellman sending the ciphertext

$$(pk_H, enc_m) = (9, 8)$$

to Alice. Compute Alice and Hellman's shared secret.

4. Let φ be the Euler φ-function. Prove that:

(a) If p is prime, the $\varphi(p) = p - 1$.

(b) If p and q are distinct primes, then $\varphi(pq) = (p - 1)(q - 1)$.

(c) If p is prime, then $\varphi(p^2) = p(p - 1)$.

5. (a) Using Euclid's algorithm, find integers a and b such that $29a+101b = 1$.

(b) Find $x \pmod{29 \cdot 101}$ such that

$$\begin{aligned} x &\equiv 5 \pmod{29} \\ x &\equiv 12 \pmod{101}. \end{aligned}$$

Recall that x exists by the Chinese Remainder Theorem.

6. This questions is a toy example of RSA. You are reommended to use a computer to aid your calculations. If you are not comfortable with programming then please use Wolfram Alpha (`www.wolframalpha.com`), or better, install SageMath `www.sagemath.org` (ask if you want help using SageMath). Set $p = 307$, $q = 311$, and $n = p \cdot q$. Note that p and q are prime numbers.

(a) Compute the RSA secret key corresponding to the RSA public key $(247, n)$.

(b) The values $m_0, m_1, m_2, m_3, m_4, m_5, m_6, m_7$ below are a message that has been encrypted using the public RSA key $(247, n)$. Decrypt this message and translate it into plaintext by assigning the value 00 to

A, 01 to B, etc., up to 25 to Z, and assigning the value 26 to !.

$$\begin{aligned} m_0 &= 94755 \\ m_1 &= 87565 \\ m_2 &= 41862 \\ m_3 &= 49231 \\ m_4 &= 34234 \\ m_5 &= 17479 \\ m_6 &= 26771 \\ m_7 &= 87503. \end{aligned}$$

(c) Give 2 examples of an invalid public key. Justify your answer.

Cryptology - Week 3 Worksheet

Question 1 is about double-and-add. Questions 2 and 3 are about groups. Question 4 is about Pohlig-Helmman. Question 5 is about extending Diffie-Hellman to a more abstract (post-quantum) setting. Starred exercises are harder exercises.

1. (a) Using double-and-add, compute $69 \cdot 73 \pmod{1000}$. Write out your steps and compute the number of additions required. (Hint: the binary expansion of 69 is 1000101).

   (b)* How would you efficiently compute $2047 \cdot 7879$?

2. From this point on, we will write

   - $\mathbb{Z}/n\mathbb{Z}$ to denote the set of integers modulo n.
   - $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ to denote the set of integers modulo p when p is a prime.
   - $\mathbb{F}_p^* = \mathbb{Z}/p\mathbb{Z} - \{0 \pmod{p}\}$ to denote the set of non-zero integers modulo p when p is a prime.

   Determine whether or not each of the following are groups G under $*$:

   (a) $G = \mathbb{R}$ and $* = +$ (addition).

   (b) $G = \mathbb{C}$ and $* = \times$ (multiplication).

   (c) $G = \mathbb{Z}/4\mathbb{Z}$ and $* = + \pmod{4}$ (addition mod 4).

   (d) $G = \mathbb{Z}/4\mathbb{Z} - \{0 \pmod{4}\}$ and $* = \times \pmod{4}$ (multiplication mod 4).

   (e) $G = \mathbb{F}_5^*$ and $* = \times \pmod{5}$ (multiplication mod 5).

   (f) $G = \mathbb{F}_p^*$, for p prime, and $* = \times \pmod{p}$ (multiplication mod p). Hint: use Fermat's Little Theorem.

3. (a) Determine whether or not $4 \pmod{5}$ is a generator for the group $\mathbb{F}_5^*$ under operation $* = \times \pmod{5}$.

   (b) Give a generator for the group $\mathbb{F}_{11}^*$ under operation $* = \times \pmod{11}$.

(c) Diffie and Hellman agree to use $p = 37$ as their prime modulus. Exactly one of the following:

$$36, 6, 5$$

is an appropriate choice for the public parameter $g \pmod{p}$. Which is it?

4. Use Pohlig-Hellman to compute $a \in \mathbb{Z}$ such that $7^a \equiv 1004 \pmod{2593}$.

5.* Suppose that G is a group with group operation $*$ and S is a set. We say that G *acts* on S if there exists a map

$$f : G \times S \to S$$

such that

- For every $g, h \in G$ and $s \in S$, we have that $f(g * h, s) = f(g, f(h, s))$.
- For every $s \in S$, if id is the identity of G then $f(id, s) = s$.

Construct a Diffie-Hellman-style key exchange algorithm in which the public keys and shared secret are elements of a set S with no known group structure, and the secret keys are elements of a commutative group G that acts on S.

Note: This should be a construction that works for any G and S – you do not have to find a specific group action.

(Fun fact: this is one method of translating the Diffie-Hellman key exchange into a protocol which cannot be broken by Shor's algorithm, since the public keys are no longer elements of a (commutative) group).

Cryptology - Week 7 worksheet

Question 1 and 2 are about RSA signatures. Question 3 is about ElGamal signatures. Question 4 is about using SageMath for modular arithmetic. Question 5 is about Pohlig-Hellman using SageMath. Download SageMath here for free: `www.sagemath.org`. Starred exercises are harder exercises.

1. Fix RSA parameters $p = 307$, $q = 311$, $n = p \cdot q$, public key $\mathrm{pk} = (247, n)$, and secret key $\mathrm{sk} = (55303, n)$. Use square-and-multiply to sign the message $m \equiv 2 \pmod{n}$.

2. Suppose that you see in the public database that a message $m \equiv 2 \pmod{110107021}$ has been signed as

$$(\mathrm{sig}, \mathrm{pk}) = (33554432, (8806881, 110107021)).$$

   (a) Without computing $\varphi(110107021)$, sign the message

$$m \equiv 6172 \pmod{110107021}$$

   as if you are the owner this RSA key. (You are advised to use a computer for this exercise, but it is possible to do by hand).

   (b) If the RSA secret key is chosen randomly, on average how long will it take an adversary using brute force to find the secret key given only the public information?

   (c)* What is the chance that a randomly chosen secret key is small enough that an adversary will find it by brute force in $\leq \log(p)$ multiplications?

   (d)* Can you think of any ways to speed up the brute-force search?

3. This question is about ElGamal signatures. Our public setup parameters will be $p = 37$ and $g = 2$.

   (a) You observe two parties claiming the identity with public key $g^a = 23$. In order to check which party is honest (if any), you ask both parties to sign the message $m \equiv 1 \pmod{36}$. You receive the signatures

$$(r_a, sig_a) = (25, 13)$$

   from party A and

$$(r_b, sig_b) = (30, 6)$$

   from party B. Check which of these parties is honest.

(b) An honest party with public key 23 signs message $m_1 = 14 \pmod{36}$ with the signature

$$(r_1, sig_1) = (19, 19)$$

and $m_2 = 4 \pmod{36}$ with the signature

$$(r_2, sig_2) = (19, 29).$$

Sign a message $m_3 = 25 \pmod{36}$ as if you are the person with public key 23.

4. You should use SageMath for this question.

(a) The command for '$n \pmod{p}$' in SageMath is '$n \,\%\, p$'. By checking all the possible values of $2^a \pmod{31}$, show that 2 does not generate $\mathbb{F}_{31}^*$ as a multiplicative group.

(b) Find a generator of $\mathbb{F}_{31}^*$ as a multiplicative group.

(c)* How many possible choices of generator are there for $\mathbb{F}_{31}^*$?

5.* By implementing Pohlig-Hellman in SageMath, compute a such that

$$11^a \equiv 8080 \pmod{12289}.$$

Cryptology - Week 8 worksheet

Questions 1-2 are about generic algorithms for the Discrete Logarithm Problem. Question 3 is about index calculus. Questions 4 and 5 are about the additional content on finite fields (only for students attepting to get a mark in the range 90-100). You should use SageMath to aid your calculations.

1. This question is about baby-step-giant-step.
   - (a) Use (only) baby-step-giant-step to compute $a \in \mathbb{Z}$ such that $9^a \equiv 17 \pmod{101}$. You may use without proof that 9 has order 50 in the multiplicative group $\mathbb{F}_{101}^*$.
   - (b) Using SageMath, check that 3 is a generator of $\mathbb{F}_{14657}^*$.
   - (c) Using SageMath and baby-step-giant-step, compute a in $\mathbb{Z}$ such that $3^a = 3441 \pmod{14657}$.
   - (d) Which extra step could you add to parts (a) and (c) before applying baby-step-giant-step to find a more efficiently?
2. (a) Use (only) Pollard-ρ to compute $a \in \mathbb{Z}$ such that $3^a \equiv 8 \pmod{17}$.
   - (b) Using SageMath, find the order of 4 in $\mathbb{F}_{1019}^*$.
   - (c) Using SageMath and Pollard-rho, compute a in $\mathbb{Z}$ such that $4^a = 78 \pmod{1019}$.
3. (a) Using index calculus and a factor base of $\{2, 3, 5\}$, find a such that $31^a \equiv 39 \pmod{107}$.
   - (b)* How would you alter the algorithm as given in the lecture notes to include a non ad-hoc way of choosing a factor base?

4.* For every finite field, there exists an *irreducible* polynomial $f(x)$ with coefficients in $\mathbb{Z}/p\mathbb{Z}$ such that

$$\mathbb{F}_{p^n} = \left\{ \sum_{i=0}^{n} c_i \alpha^i : c_i \in \mathbb{Z}/p\mathbb{Z} \text{ and } f(\alpha) \equiv 0 \pmod{p} \right\}$$

. Which of the following are valid choices of p and $f(x)$?

(a) $p = 2$ and $f(x) = x^2 + x + 1$.

(b) $p = 2$ and $f(x) = x^2$.

(c) $p = 3$ and $f(x) = x^2 + x + 1$.

(d) $p = 3$ and $f(x) = x^3 + 2$.

5.* Consider the finite field

$$\mathbb{F}_{2^9} = \left\{ \sum_{i=0}^{8} a_i x^i : a_i \in \mathbb{Z}/2\mathbb{Z},\ x^9 + x^4 + 1 \equiv 0 \pmod 2 \right\}.$$

Let $g = x$; then g generates $\mathbb{F}_{2^9}^*$ as a multiplicative group (you do not have to prove this).

Using index calculus with a factor base of

$$\{x + 1, x^4 + x + 1, x^2 + x + 1\},$$

compute $a \pmod{2^9 - 1}$ such that $g^a = x^4 + x$.

Cryptology
Selected Model Solutions

This is a set of model solutions to the exercises that have been requested from the sheets for weeks 2, 3, and 7.

[Week 2, Q2c]

(c) [This question was mostly intended for you to start to come up with Pohlig-Hellman on your own.] The Chinese Remainder Theorem tells us that if we know $\mathrm{sk}_H \pmod 4$ and $\mathrm{sk}_H \pmod 9$, then it is uniquely defined mod $36 = 4 \cdot 9$, which by part (b) is sufficient.

To compute $\mathrm{sk}_H \pmod 4$, we need to find $h_0 \in \{0, 1, 2, 3\}$ such that there exists m with $\mathrm{sk}_H = h_0 + 4m$; that is, h_0 such that $g^{h_0+4m} = g^{h_0} \cdot (g^4)^m = 5$. If we raise this equation to the power of 9 ($= 36/4$), that gives us

$$6 = 5^9 = g^{9h_0} \cdot (g^{36})^m = (g^9)^{h_0} \cdot 1 = 31^{h_0} \pmod{37},$$

where the second equality follows from Fermat's Little Theorem. Checking through the options $h_0 = 0, 1, 2, 3$ we find that the above equation is satisfied only when $h_0 = 3$, so $\mathrm{sk}_H \equiv 3 \pmod 4$.

We now follow a similar process to compute $h \pmod 9$. We need to find $h_1 \in \{0, \ldots, 8\}$ such that there exists m' with $\mathrm{sk}_H = h_1 + 4m'$; that is, h_1 such that $g^{h_1+4m'} = g^{h_1} \cdot (g^9)^{m'} = 5$. If we raise this equation to the power of 4 ($= 36/9$), that gives us

$$33 = 5^4 = g^{4h_1} \cdot (g^{36})^{m'} = (g^4)^{h_1} \cdot 1 = 16^{h_1} \pmod{37},$$

where the second equality follows from Fermat's Little Theorem. Checking through the options $h_1 = 0, 1, \ldots, 8$ we find that the above equation is satisfied only when $h_1 = 5$, hence $\mathrm{sk}_H \equiv 5 \pmod 9$.

Finally, we could run Euclid's algorithm to find $\mathrm{sk}_H \pmod{36}$ given that $\mathrm{sk}_H \equiv 3 \pmod 4$ and $\mathrm{sk}_H \equiv 5 \pmod 9$, but we can also just observe that $\mathrm{sk}_H = 23 \pmod{36}$ is the (necessarily unique) solution. As a sanity check, we check that $2^{23} \equiv 5 \pmod{37}$.

[Week 3, Q5] For the setup information, we fix an element $s_0 \in S$. User A initiates a randomly chosen secret key $a \in G$ and computes and publishes their public key $\mathrm{pk}_A = f(a, s_0)$ (this is an element of S). Similarly, User B initiates a randomly chosen secret key $b \in G$ and computes and publishes their public key $\mathrm{pk}_B = f(b, s_0)$. Then, User A computes the shared secret key as $\mathrm{ssk} = f(a, \mathrm{pk}_B)$ and User B computes the shared secret key as $\mathrm{ssk} = f(b, \mathrm{pk}_A)$. Observe that

$$f(a, \mathrm{pk}_B) = f(a, f(b, s_0)) = f(a{*}b, s_0) = f(b{*}a, s_0) = f(b, f(a, s_0)) = f(b, \mathrm{pk}_A),$$

so this is indeed a valid cryptosystem.

[Week 7, Q2d]

(d) [This question was intended to nudge you to come up with baby-step-giant-step ideas on your own. Note that brute-forcing the secret key means trying every option for the secret key, typically in order, until you find the one that makes the public key.]

[Week 7, Q3b]

(b) The owner of the public key 23 has reused their nonce k since $r_1 = r_2$ and r is defined as g^k. Therefore I can recover their secret key: write $r_1 = r_2 = g^k$. By definition

$$sig_1 \equiv k^{-1}(m_1 - r \cdot \mathrm{sk}) \pmod{p-1}$$

and

$$sig_2 \equiv k^{-1}(m_2 - r \cdot \mathrm{sk}) \pmod{p-1}.$$

Solving these two equations for k gives

$$k \equiv \frac{m_1 - m_2}{sig_1 - sig_2} \equiv \frac{10}{-10} \pmod{36}.$$

Now 10 is not invertible $\pmod{36}$, so this equation has multiple solutions, but let us try $k = -1$. (If k is not -1, we can try the other value for k satisfying the equation $-2k \equiv 2 \pmod{36}$–note that dividing by 5 is no problem–namely $k = 17$.) This would give

$$\mathrm{sk} \equiv r_1^{-1}(m_1 - k \cdot sig_1) \equiv 19 \cdot (14 + 19) \equiv 15 \pmod{36}.$$

Check: $2^{15} \equiv 23$, so this is indeed the secret key. Now to sign the message, I will use a new randomly chosen nonce $k = 19$, giving $r \equiv 2^{19} \equiv 35 \pmod{37}$. Then

$$sig \equiv k^{-1}(m - ar) \equiv 19 \cdot (25 - 15 \cdot 35) \equiv 4 \pmod{36}.$$

So I sign the message as $(r, sig) = (35, 4)$.