MT3660/4660/5466
Cryptography II
Problem Sheet 1

To be submitted by midnight on Monday 25 January 2021.

Attempt every question. Please remember to write your name or student number. The eight problem sheets are worth 15% of the final mark.

1. Let p and q be odd primes with $p \neq q$, and let $n = pq$. Show that there are four distinct solutions x (modulo n) to the equation $x^2 = 1 \bmod n$.

2. The Carmichael lambda function $\lambda(n)$ for a positive integer n is defined to be the smallest positive integer m such that $g^m = 1$ for all $g \in \mathbb{Z}_n^*$, where $\mathbb{Z}_n^* = \{x \in \{1, \ldots, n-1\} | x \text{ and } n \text{ coprime}\}$.

   (a) Prove that $\lambda(n)$ divides $\varphi(n)$.

   (b) Show that if $n = pq$ is a product of two distinct odd primes then $\lambda(n) \leq \varphi(n)/2$.

   (c) Let (N, e) be an RSA public key. Prove that if $d \in \mathbb{N}$ satisfies $ed = 1 \pmod{\lambda(N)}$ then RSA decryption using d works.

3. Let $N = pq$ be a product of two odd primes. Show that the factorisation of N can be found efficiently if the value of $\varphi(N)$ is known.

4. Give a formal description (including a specification of the form of the input and output) of the problem solved by the extended Euclidean algorithm.

5. Consider the INEQUALITY problem stated below.

   Problem: INEQUALITY
   Input: Two k-bit integers a and b.
   Output: The answer to the following question. Does $a \leq b$ hold?

   Show that there exists an $O(k)$ algorithm to solve this INEQUALITY problem. Give a brief justification to show that the complexity of this algorithm is $O(k)$.

MT3660/4660/5466
Cryptography II
Problem Sheet 2

To be submitted by midnight on Monday 1 February 2021.

Attempt every question. Please remember to write your name or student number. The eight problem sheets are worth 15% of the final mark.

1. Why is trial division an exponential algorithm?

2. Let G be a graph with n vertices. A *clique* of size k is a set of k vertices of G all connected to each other. A *vertex cover* of G is a set X of vertices of G such that every edge of G has one or both of its end-points in X. The *complement* G^c of G has the same vertex set as G, and there is an edge between two vertices in G^c if and only if there is no edge between these vertices in G.

   (a) Show that G has a clique of size k if and only if its complement G^c has a vertex cover of size $n - k$.

   (b) Consider the VERTEX COVER problem.
   Input: a graph G and an integer k.
   Output: The answer to: Does G have a vertex cover of size k?

   Show that CLIQUE $\leq_T$ VERTEX COVER.

3. Compute (by hand) the following Jacobi symbols.

$$\text{(a)} \ \left(\frac{101}{203}\right). \qquad \text{(b)} \ \left(\frac{67}{451}\right). \qquad \text{(c)} \ \left(\frac{103}{135}\right).$$

4. The ACME software company has produced an RSA encryption package. You notice that this software performs decryption extremely fast, and you suspect this may be because the decryption exponent d has been chosen to be very small.

   Your competitor has been foolish enough to purchase this software and you have obtained a ciphertext c sent to them. The public key and the ciphertext are available on the file `ACME-TW02.txt` on Moodle. Decrypt this ciphertext.

   Write the message on your solution sheet (or print the Mathematica output). [The Mathematica function `PowerMod` is useful.]

MT3660/4660/5466
Cryptography II
Problem Sheet 3

To be submitted by midnight on Monday 8 February 2021.

Attempt every question. Please remember to write your name or student number. The eight problem sheets are worth 15% of the final mark.

1. Why does the Textbook RSA cryptosystem not possess the One Way Encryption (OWE) property under a CCA2 attack?

2. Suppose we use an RSA signature scheme without a hash function or message padding, so a message $m \in \mathbb{Z}_N^*$ is signed by computing the signature $s = m^d \pmod N$.

   (a) Is this scheme secure against selective forgery or existential forgery in a passive attack model?

   (b) What about in the adaptive chosen-message attack model?

3. Let (`KeyGen`, `Sign`, `Verify`) be a signature scheme.

   (a) Give a formal definition (Adversary A inputs/outputs, a game and success criterion) of selective forgery in a passive attack model.

   (b) Given a formal definition (same information as (a)) of existential forgery in a passive attack model.

4. The file `Rabin-ProbSheet3.txt` on the course Moodle page contains a Rabin modulus n and primes p and q with $n = pq$.

   (a) The ciphertext cA in `Rabin.txt` is obtained by using a Rabin encryption with Redundancy Scheme A. Find the corresponding message. (You can print the Mathematica output.)

   (b) The ciphertext cB in `Rabin.txt` is obtained by using a Rabin encryption with Redundancy Scheme B in which a message is padded by appending ten 0s before modular squaring. Find the corresponding message. (You can print the Mathematica output.)

5. Suppose that p and q are primes such that $p, q = 3 \bmod 4$ and let $n = pq$. If m is an integer with Jacobi symbol $\left(\frac{m}{n}\right) = 1$, then show that either m or $-m$ is a square modulo n.
[**Note**. This result is required for Redundancy Scheme A to work.]

MT3660/4660/5466
Cryptography II
Problem Sheet 4

To be submitted by midnight on Monday 22 February 2021.

Attempt every question. Please remember to write your name or student number. The eight problem sheets are worth 15% of the final mark.

1. ACME software builds RSA modulus $N = pq$ by choosing a random k-bit prime p and then setting
$$\mathtt{q} = \mathtt{NextPrime}[\mathtt{p}+1].$$
The file `ACME2-ProbSheet4` on the course Moodle page contains such a public key. Compute the private key for this example and hence the message m corresponding to the given ciphertext. Either write down or include a printout of the message.

2. Consider a related message attack on Textbook RSA with modulus N and public exponent $e = 3$, in which the related messages $m_0 = x$ and $m_1 = x + 1$ are encrypted to give c_0 and c_1 respectively.
   (a) Show that x satisfies $(c_1 - c_0 + 2)x - (c_1 + 2c_0 - 1) = 0 \bmod N$.
   (b) The file `RelMess-ProbSheet4` on Moodle contains an RSA modulus N and ciphertexts c_0 and c_1 corresponding to the encryptions of such related messages m_0 and $m_1 = m_0 + 1$. Find these two messages m_0 and m_1.

3. The file `Wiener-ProbSheet4` on Moodle contains an RSA public key such that the corresponding private key d is relatively small. Use the small private exponent method (Wiener's algorithm) to compute d.

   Note. The solution should arise after less than 10 iterations of Euclid's method, so this problem can be done by hand or using Mathematica.

4. Two users have Rabin public keys $N_1 = 144946313$ and $N_2 = 138951937$. The same message m is encrypted using padding scheme A to the 2 users, giving ciphertexts
$$c_1 = (48806038, -1, 1) \text{ and } c_2 = (14277753, -1, 1).$$
Use the Håstad attack to find the corresponding message.

5. Consider the following signature scheme based on RSA. The public key is an integer $N = pq$, an integer e coprime to $\lambda(N)$ and an integer a such that $\gcd(a, N) = 1$. The private key is the inverse of e modulo $\lambda(N)$ as usual. Let H be a collision-resistant hash function. The signature on a message m is a residue s such that

$$s^e = a^{H(m)} \pmod{N}$$

where $H(m)$ is interpreted as an integer.

(a) Explain how the signer can generate signatures efficiently.

(b) Find a known message attack on this system which allows an adversary to make selective forgery of signatures.

Hint. Start by assuming that you are given signed messages m_1 and m_2, where $H(m_1)$ and $H(m_2)$ are coprime.

MT3660/4660/5466
Cryptography II
Problem Sheet 5

To be submitted by midnight on Monday 1 March 2021.

Attempt every question. Please remember to write your name or student number. The eight problem sheets are worth 15% of the final mark.

Clarification. Question 5(b) as expressed below is not correct, so Questions 5(b) and 5(c) will not count as part of the formal Problem Sheet 5 assessment. An amended version of Question 5 is given overleaf.

1. Consider the set $A = \{1, \theta, \theta + 1, \theta^2, \theta^2 + 1, \theta^2 + \theta, \theta^2 + \theta + 1\}$.
   (a) Show that A is a cyclic group under polynomial multiplication, where polynomials are reduced modulo 2 and modulo $\theta^3 + \theta + 1$.
   (b) Find an integer k such that $\theta^k = \theta^2 + \theta + 1$ in A.
2. Find an integer x such that $731^x = 464 \bmod 1103$ by using the Silver-Pohlig-Hellman discrete logarithm method. (You may assume that the order of 731 modulo 1103 is 551.)
3. Find an integer x such that $59^x = 5 \bmod 107$ by using the Baby-Step-Giant-Step discrete logarithm method.
4. Find an integer x such that $262^x = 113 \bmod 569$ by using the Pollard Rho discrete logarithm method. (You may assume that the order of 262 modulo 569 is 71.)
5. (a) Find the order of 23 modulo 479 (prime).
   (b) Use the ideas of Index Calculus to show that

$$\begin{pmatrix} 2 \\ 3 \\ 5 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 2 \\ 6 & 1 & 0 \\ 2 & 0 & 1 \end{pmatrix} \begin{pmatrix} \log_{23} 2 \\ \log_{23} 3 \\ \log_{23} 5 \end{pmatrix} \mod 478.$$

   (c) Find an integer x such that $453 = 23^x \bmod 479$.

You may assume that $\begin{pmatrix} 1 & 0 & 2 \\ 6 & 1 & 0 \\ 2 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 159 & 0 & 160 \\ 2 & 1 & 474 \\ 160 & 0 & 159 \end{pmatrix} \mod 478.$

Amended Question 5. Comments will be provided on any submitted solution to Amended Question 5(b) and 5(c), though these are not counted as part of formal assessment. It is not necessary to attempt revised part (b) and part (c), for example if you had already submitted Solutions before this Amended Question 5 was issued.

Q5 Part (a). Find the order of 23 modulo 479 (prime).

Q5 Part (b) (*Amended*). Use the ideas of Index Calculus to show that

$$\begin{pmatrix} 241 \\ 242 \\ 244 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 2 \\ 6 & 1 & 0 \\ 2 & 0 & 1 \end{pmatrix} \begin{pmatrix} \log_{23} 2 \\ \log_{23} 3 \\ \log_{23} 5 \end{pmatrix} \quad \text{mod } 478.$$

You may assume that $23^{241} = 50$, $23^{242} = 192$, $23^{244} = 20 \text{ mod } 479$.

Q5 Part (c). Find an integer x such that $453 = 23^x \text{ mod } 479$.

You may assume that $\begin{pmatrix} 1 & 0 & 2 \\ 6 & 1 & 0 \\ 2 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 159 & 0 & 160 \\ 2 & 1 & 474 \\ 160 & 0 & 159 \end{pmatrix} \text{ mod } 478.$

MT3660/4660/5466
Cryptography II
Problem Sheet 6

To be submitted by midnight on Monday 15 March 2021.

Attempt every question. Please remember to write your name or student number. The eight problem sheets are worth 15% of the final mark.

1. Let $\mathcal{L}$ be the lattice generated by the linearly independent 2-dimensional vectors $u, v \in \mathbb{R}^2$, and let θ be the angle between u and v.

   (a) Show that $\text{Vol}(\mathcal{L}) = \|u\| \, \|v\| \, |\sin\theta|$.

   (b) Show that the product $\|u\| \, \|v\|$ over all choices $\{u, v\}$ of basis for $\mathcal{L}$ is minimised when the angle θ is closest to $\pm\frac{1}{2}\pi$.

2. Consider the lattice $\mathcal{L}$ generated by the basis vectors

$$b_1 = (2, 6, 4) \ , \quad b_2 = (5, 1, -4) \ \text{ and } \ b_3 = (3, -3, 3).$$

   (a) Show that the basis vectors b_1, b_2 and b_3 are orthogonal.

   (b) Explain why $\text{Vol}(\mathcal{L})$ is equal to $|b_1| \times |b_2| \times |b_3|$.

   (c) Find a smallest vector in the lattice $\mathcal{L}$.

   (d) Find $\lambda_1, \lambda_2, \lambda_3$ such that $(66, -56, -47) = \lambda_1 b_1 + \lambda_2 b_2 + \lambda_3 b_3$.

   (e) Find the closest vector in the lattice $\mathcal{L}$ to the vector $(66, -56, -47)$.

3. Consider the lattice $\mathcal{L}$ generated by basis matix $B = \begin{pmatrix} 125 & 212 \\ 39 & 66 \end{pmatrix}$.

   (a) The matrix $B' = \begin{pmatrix} 8 & 14 \\ 39 & 66 \end{pmatrix}$ is obtained by applying the elementary row operation Row 1 → Row 1 − 3 × Row 2 to B. Explain why the lattice generated by the basis matrix B' is the lattice $\mathcal{L}$.

   (b) By applying a series of similar elementary row operations to the matrix B', find a basis matrix B'' for the lattice $\mathcal{L}$ in which every entry B''_{ij} has absolute size at most 4, that is to say $|B''_{ij}| \leq 4$.

   (c) Find a shortest vector in the lattice $\mathcal{L}$.

   (d) Find the closest vector in the lattice $\mathcal{L}$ to the vector $(-5, 5)$.

4. Consider the lattice $\mathcal{L}$ with basis matrix

$$B = \begin{pmatrix} 76 & -90 & 98 & -69 & 47 \\ -21 & -95 & -63 & -83 & -88 \\ -19 & 92 & 82 & -27 & 82 \\ -90 & 47 & 2 & -43 & 95 \\ 86 & -99 & 10 & 38 & 44 \end{pmatrix}.$$

(a) Find a vector $v \in \mathcal{L}$ with $|v| < 60$.

(b) Find the closest vector v in the lattice $\mathcal{L}$ to the vector

$$w = (-1920, 2562, -458, -1358, -2111).$$

(c) Find an integer vector z sucht that $|w - zB| < 4$.

You may include Mathematica output as appropriate in your solutions.

MT3660/4660/5466
Cryptography II
Problem Sheet 7

To be submitted by midnight on Monday 22 March 2021.

Attempt every question. Please remember to write your name or student number. The eight problem sheets are worth 15% of the final mark.

1. A GGH cryptosystem has the lattice basis matrix $B = \begin{pmatrix} 7 & 0 \\ 0 & 9 \end{pmatrix}$ and unimodular matrix $U = \begin{pmatrix} 5 & 7 \\ 2 & 3 \end{pmatrix}$ as its private key.

   (a) Find the corresponding public key matrix B' and encrypt the message $m = (3, 5)$ using error $e = (1, -1)$.

   (b) Decrypt the ciphertext $c = (-109, -32)$.

2. A GGH cryptosystem based on a lattice $\mathcal{L}$ with public key basis matrix

$$B' = \begin{pmatrix} 53 & 67 & -5 & -26 & -92 & -148 \\ 106 & 201 & 5 & -65 & -69 & -222 \\ -159 & -402 & -25 & 65 & -138 & 37 \\ -159 & -335 & -30 & 273 & 161 & 888 \\ 0 & -335 & -95 & 286 & -368 & 555 \\ -159 & -536 & -65 & 221 & -506 & -222 \end{pmatrix}$$

   has a plaintext m encrypted to give ciphertext

$$c = (-1376, -4553, -607, 2496, -2667, 2815).$$

   (a) Show that Babai rounding of c for the lattice $\mathcal{L}$ with the public key matrix B' gives lattice point

$$(-1537, -4958, -640, 2652, -2737, 3145).$$

   (b) Find a candidate private key matrix B. (This is not unique.)

   (c) Find the closest vector to c in the lattice $\mathcal{L}$.

   (d) Find the message m encrypted by B' to give c.

3. Consider the LWE Problem of the form $b = As + e \bmod q$, given by

$$\begin{pmatrix} 534 \\ 602 \\ 274 \\ 447 \end{pmatrix} = \begin{pmatrix} 446 & 269 \\ 399 & 400 \\ 633 & 699 \\ 302 & 393 \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \end{pmatrix} + \begin{pmatrix} e_1 \\ e_2 \\ e_3 \\ e_4 \end{pmatrix} \qquad \text{mod } 787,$$

where b, A and q are given in the above equation, and the components of e have a rounded Normal $[\mathrm{N}(0, 2.0^2)]$ distribution.

(a) Find a basis for the 4-dimensional q-ary lattice $\mathcal{L}$ generated by A.

(b) Find the nearest vector in $\mathcal{L}$ to b.

(c) Find the secret $s = (s_1, s_2)^T$.

4. Consider an LWE cryptosystem based on the LWE Problem given in Question 3, that is to say with public key

$$A = \begin{pmatrix} 446 & 269 \\ 399 & 400 \\ 633 & 699 \\ 302 & 393 \end{pmatrix} \qquad \text{and} \qquad b = \begin{pmatrix} 534 \\ 602 \\ 274 \\ 447 \end{pmatrix} \qquad \text{modulo } q = 787.$$

(a) Encrypt the bit $\theta = 1$ using the public key (A, b) and the random binary vector $x = (1, 0, 0, 1)^T$.

(b) Decrypt the ciphertext $v = (691, 581)$ and $w = 623$ with the random binary vector $x = (1, 1, 1, 0)^T$.

MT3660/4660/5466
Cryptography II
Problem Sheet 8 – Revised

To be submitted by midnight on Monday 29 March 2021.

Attempt every question. Please remember to write your name or student number. The eight problem sheets are worth 15% of the final mark.

Note. The webpage `https://graui.de/code/elliptic2/` gives a convenient **Elliptic Curve Tool** for generating the Addition Table and related information for an elliptic curve group over a finite field $\mathbb{F}_p$. Clicking an elliptic curve point on the graph gives further information about that point.

1. Consider the elliptic curve $y^2 = x^3 + ax + b$ over a finite field $\mathbb{F}_p$ with $p > 3$ and formal partial derivatives $2y$ and $3x^2 + a$.

   (a) Consider the elliptic curve point $P = (x_P, y_P)$ on this curve. Explain why $(x - x_P)$ is a factor of both $x^3 + ax + b$ and $3x^2 + a$ if and only if both formal derivatives vanish at P.

   (b) Show that both formal partial derivatives for the curve $y^2 = x^3$ in $\mathbb{F}_p$ vanish at the elliptic curve point $P = (0, 0)$.

   (c) Show that there is no elliptic curve point $P = (x_P, y_P)$ on the elliptic curve $y^2 = x^3 + b$ over $\mathbb{F}_p$ at which both formal derivatives vanish.

   (d) If $a \neq 0$ in the elliptic curve $y^2 = x^3 + ax + b$ over $\mathbb{F}_p$ and using the notation $\frac{3}{2a}$ to mean $3(2a)^{-1}$ in $\mathbb{F}_p$ and so on, then show that

$$\begin{aligned} x^3 + ax + b &= \frac{1}{3}x(3x^2 + a) + \left(\frac{2a}{3}x + b\right) \\ &= \left(\frac{3}{2a}x^2 - \frac{9b}{4a^2}x + 1\right)\left(\frac{2a}{3}x + b\right) + \frac{1}{3}x\left(a + \frac{27b^2}{4a^2}\right) \end{aligned}$$

   and that

$$3x^2 + a = \left(\frac{9}{2a}x - \frac{27b}{4a^2}\right)\left(\frac{2a}{3}x + b\right) + \left(a + \frac{27b^2}{4a^2}\right).$$

   (e) Show that the elliptic curve $y^2 = x^3 + ax + b$ over a finite field $\mathbb{F}_p$ with $p > 3$ is singular if and only if $4a^3 + 27b^2 = 0 \bmod p$.

2. Consider the elliptic curve group $E(\mathbb{F}_7)\colon y^2 = x^3 + 3x + 5$.

   (a) Complete the following Table in order to enumerate $E(\mathbb{F}_7)$.

x	0	1	2	3	4	5	6
x^3	0	1					
$3x$	0	3					
5	5	5	5	5	5	5	5
y^2	5	2					
y	**X**	3, 4					

   Write down the set of elements of $E(\mathbb{F}_7)$ and state the group isomorphism class of $E(\mathbb{F}_7)$ (C_n or $C_n \times C_m$ for specified n and m).

   (b) The line $\ell\colon y = 2x + 1$ intersects $E(\mathbb{F}_7)$ at $(1, 3)$ and $(6, 6)$. Find the third point of intersection of ℓ and $E(\mathbb{F}_7)$. Hence give the elliptic curve point sum $(1, 3) + (6, 6)$ in $E(\mathbb{F}_7)$.

   (c) The line $\ell'\colon y = x + 2$ intersects $E(\mathbb{F}_7)$ at $(1, 3)$ and $(6, 1)$. Find all points of intersection (giving multiplicities) of ℓ and $E(\mathbb{F}_7)$. Hence find the elliptic curve point doubling $[2](1, 3) = (1, 3)+(1, 3)$ in $E(\mathbb{F}_7)$. GIve reasons.

   (d) Find an integer k such that $[k](1, 3) = (6, 1)$ in $E(\mathbb{F}_7)$.

3. Consider the elliptic curve group $E(\mathbb{F}_{43})\colon y^2 = x^3 + 2x + 4$. An Elliptic Curve Diffie-Hellman scheme in $E(\mathbb{F}_{43})$ is constructed with base point $P = (0, 2)$ with order 49, in which Alice and Bob have private key integers x_A and x_B respectively elliptic curve public key points

$$\begin{aligned} Q_A &= (14, 14) = [x_A]P = [x_A](0, 2) \\ \text{and} \quad Q_B &= (35, 11) = [x_B]P = [x_B](0, 2) \quad \text{respectively.} \end{aligned}$$

   Find Alice and Bob's shared secret elliptic curve point

$$[x_A x_B]P = [x_A x_B](0, 2).$$

   Note. You may use without proof any result from the *Elliptic Curve Tool* for this Question.

4. Consider the elliptic curve group $E(\mathbb{F}_{37})\colon y^2 = x^3 + 5x + 11$ with 31 points. Consider the Elliptic Curve Discrete Logarithm Problem in $E(\mathbb{F}_{37})$ given by $Q = [k]P$ with $P = (0, 14)$ and $Q = (10, 5)$, that is to say find k such that $(10, 5) = [k](0, 14)$.

   (a) Let $R = -[6]P = [25](0, 14) = (25, 6) \in E(\mathbb{F}_{37})$. Complete the following Table

	0	1	2	3	4	5
$[i]P$	$\mathcal{O}$	$(0, 14)$	$(30, 15)$	$(4, 13)$		
$[j]R$	$\mathcal{O}$	$(25, 6)$	$(21, 4)$	$(19, 34)$		
$Q + [j]R$	$(10, 5)$	$(27, 21)$	$(32, 34)$	$(33, 36)$		

   (b) Show how to use the above (completed) Table with the Baby-Step Giant-Step approach to compute k such that $(10, 5) = [k](0, 14)$.

   (c) An Elliptic Curve Diiffie-Hellman scheme is constructed in $E(\mathbb{F}_{37})$ with base point $P = (0, 14)$ and in which Alice and Bob have public key elliptic curve points $Q_A = (10, 5)$ and $Q_B = (32, 3)$ (see Question 3). What is Alice and Bob's shared secret elliptic curve point?

Note. You may use without proof any result from the *Elliptic Curve Tool* for this Question.