# MT3660/4660/5466
# Cryptography II
# Group Work Teaching Week 1

11 January 2021

Each group will get a mark out of 2 based on engagement with the session. It is not necessary to complete all questions to obtains a mark of 2.
Do **NOT** erase your whiteboard after the session is over.

Each online group should appoint one member to keep an MS Teams chat window open using the channel for your group. Do not use audio or video on MS Teams, as MS Teams is just there for the chat function. You can use MS Chat or email to summon the lecturer when you need help.

Make sure you are signed-in and that you have associated your account with Royal Holloway using the code WVTSJYJMBNQP. Check everyone has voice communication. Click "+" at bottom right to make new slides if needed.

1. A Textbook Diffie-Hellman scheme has prime $p = 67$ and generator $g = 2$, where Alice has private key $x_A$ and public key $y_A = g^{x_A} \bmod p$ and Bob has private key $x_B$ and public key $y_B = g^{x_B} \bmod p$

   (a) Write down $g^{p-1} \bmod p$, that is to say $2^{66} \bmod 67$, giving reasons.

   (b) Write down $g^{\frac{1}{2}(p-1)} \bmod p$, that is to say $2^{33} \bmod 67$, giving reasons.

   (c) If Alice has private key $x_A = 5$ and Bob has public key $y_B = 31$, then determine the shared secret of Alice and Bob.

   (d) If Alice has public key $y_A = 55$ and Bob has public key $y_B = 31$, then determine the shared secret of Alice and Bob.

2. A Textbook RSA encryption system has modulus $N = pq = 6497$ and public key exponent $e = 5569$.

   (a) Explain why one of the primes $p$ or $q$ is less than 80.

   (b) Use trial division to find the primes $p$ and $q$.

   (c) Use the Extended Euclidean algorithm to find the private key exponent $d$ satisfying $ed = 1 \bmod \phi(N)$. [Show your working]

   (d) Find the message $m$ corresponding to the ciphertext $c = 1083$.

3. Explain why $e = 2$ cannot be used as a public key exponent in a Textbook RSA encryption system.

4. A Textbook El Gamal encryption system has prime $p = 97$, generator $g = 5$, and private key $x$ and public key $y = g^x \bmod p$ is $y = 21$. Further suppose the message $m$ gives the ciphertext $(g^k, my^k) = (60, 26)$.

   (a) Show that 2 is not a generator modulo $p$.

   (b) Find the private key $x$ given that $x \in \{1, \ldots, 10\}$.

   (c) Find $g^{-xk} \bmod p$ using the Extended Euclidean algorithm or otherwise. [Show your working]

   (d) Find the message $m$.

# MT3660/4660/5466
# Cryptography II
# Group Work Teaching Week 2

19 January 2021

Each group will get a mark out of 2 based on engagement with the session. It is not necessary to complete all questions to obtains a mark of 2.
Do **NOT** erase your whiteboard after the session is over.

Each online group should appoint one member to keep an MS Teams chat window open using the channel for your group. Do not use audio or video on MS Teams, as MS Teams is just there for the chat function. You can use MS Chat or email to summon the lecturer when you need help.

Make sure you are signed-in and that you have associated your account with Royal Holloway using the code WVTSJYJMBNQP. Check everyone has voice communication. Click "+" at bottom right to make new slides if needed.

1. A Textbook El Gamal signature system has prime $p$ and generator $g$ modulo $p$. A scheme participant has private key $x$ and public key $y = g^x \bmod p$. The signature of a (hashed) message $m \in \{1, \ldots, p-1\}$ is $(r, s)$, where

$$r = g^k \bmod p \quad \text{and} \quad s = (m - xr)k^{-1} \bmod (p-1).$$

The El Gamal signature verification verification process is to check whether $g^m$ equals $y^r r^s$ modulo $p$.

(a) Show that $g^m = y^r r^s \bmod p$ for a valid signature $(r, s)$ for a message $m$.

(b) A Textbook El Gamal signature scheme has prime $p = 131$ and generating element $g = 2$, in which Alice has private key $x = 11$. Generate a valid signature with Alice's private key for the message $m = 56$.

(c) A Textbook El Gamal signature scheme (Question 1) has prime $p = 107$ and generating element $g = 2$, in which Bob has public key $y = 23$. Find which of the following pairs are valid signatures with Bob's private key for the message $m = 37$.
(i) $(r, s) = (7, 59)$. (ii) $(r, s) = (63, 28)$. (iii) $(r, s) = (24, 81)$.

2. (a) Calculate $25^{25} \bmod 37$ using the *Square-and-Multiply* Technique.

   (b) Explain how to adapt the *Square-and-Multiply* Technique for calculating $a^x \bmod q$ to give a *Double-and-Add* Technique for calculating $x \times a \bmod q$.

   (c) Use this *Double-and-Add* Technique to calculate $25 \times 25 \bmod 37$ using only doubling and addition operations.

3. Consider the arithmetic of $n \times n$ matrices over $\mathrm{GF}(p) = \mathbb{Z}_p$ for a prime $p$, that is to say matrix arithmetic modulo $p$.

   (a) Explain why the addition $A + B$ of two such matrices $A$ and $B$ can be determined with $O(n^2)$ modulo $p$ addition operations.

   (b) Explain why the product $AB$ of two such matrices $A$ and $B$ can be determined with $O(n^3)$ modulo $p$ multiplication operations and a negligible number of modulo $p$ addition operations.

   (c) Explain why the inverse $A^{-1}$ of such an invertible matrix $A$ can be determined with $O(n^3)$ modulo $p$ multiplication operations and a negligible number of modulo $p$ addition operations.

4. Consider the division of a $k$-bit positive integer $a$ by an $l$-bit positive integer $b$ with $a > b > 0$ by a binary version of long division to produce a quotient $q$ and remainder $r$, that is to say integers $q$ and $r$ satisfying $a = qb + r$ with $0 \leq r < b$. Show that this long division algorithm requires $O(k^2)$ bit operations.

# MT3660/4660/5466
# Cryptography II
# Group Work Teaching Week 3

26 January 2021

Each group will get a mark out of 2 based on engagement with the session. It is not necessary to complete all questions to obtains a mark of 2.
Do **NOT** erase your whiteboard after the session is over.

**Change to Process**. The relevant part of Question 1 is to be attempted individually. A serious individual attempt has to be made to the relevant part in order for an individual to be awarded the overall group mark. Questions 2-4 are to be attempted as a joint effort (as in previous weeks).

Each online group should appoint one member to keep an MS Teams chat window open using the channel for your group. Do not use audio or video on MS Teams, as MS Teams is just there for the chat function. You can use MS Chat or email to summon the lecturer when you need help.

Make sure you are signed-in and that you have associated your account with Royal Holloway using the code WVTSJYJMBNQP. Check everyone has voice communication. Click "+" at bottom right to make new slides if needed.

1. **Individual**. Attempt the part corresponding to the number/position you signed the cover sheet. Thus you should attempt part (1) if you are the first signatory and so on. Please write your name by your answer.

   Evaluate the appropriate Jacobi symbol showing your working.

   (1) $\left(\dfrac{313}{589}\right)$

   (2) $\left(\dfrac{379}{551}\right)$

   (3) $\left(\dfrac{353}{629}\right)$

   (4) $\left(\dfrac{481}{621}\right)$

   (5) $\left(\dfrac{367}{513}\right)$

   (6) $\left(\dfrac{319}{527}\right)$

**Questions 2-4 are to be attempted as joint effort (as before).**

2. Find both square roots of 351 modulo 617.

3. Find both square roots of 11 modulo 137 by using the Tonelli-Shanks algorithm.

4. Consider the following two problems.

   **Problem**. FACTOR-3MOD4
   Input. Integer $N = pq$, where $p, q$ are primes satisfying $p, q = 3 \bmod 4$.
   Output. A prime factor ($p$ or $q$) of $N$.

   **Problem**. SQRT-3MOD4
   Input. Integer $N = pq$, where $p, q$ are primes satisfying $p, q = 3 \bmod 4$.
   Integer $a$ such that $a$ is a nonzero square modulo $N$
   Output. All four square roots of $a$ modulo $N$.

   (a) Given an Oracle $\mathcal{O}$ for the FACTOR-3MOD4 Problem, show how to solve the SQRT-3MOD4 Problem.

   (b) Show that SQRT-3MOD4 $\leq_T$ FACTOR-3MOD4.

   (c) Find all four square roots of 55 modulo 22657, given that the 139 is a prime factor of 22657 and that 55 is a square modulo 22657. (Check your answers.)

# MT3660/4660/5466
# Cryptography II
# Group Work Teaching Week 4

2 February 2021

Each group will get a mark out of 2 based on engagement with the session. It is not necessary to complete all questions to obtains a mark of 2.
Do **NOT** erase your whiteboard after the session is over.

**Change to Process**. The relevant part of Question 1 is to be attempted individually. A serious individual attempt has to be made to the relevant part in order for an individual to be awarded the overall group mark. Questions 2-4 are to be attempted as a joint effort (as in previous weeks).

Each online group should appoint one member to keep an MS Teams chat window open using the channel for your group. Do not use audio or video on MS Teams, as MS Teams is just there for the chat function. You can use MS Chat or email to summon the lecturer when you need help.

Make sure you are signed-in and that you have associated your account with Royal Holloway using the code WVTSJYJMBNQP. Check everyone has voice communication. Click "+" at bottom right to make new slides if needed.

1. **Individual**. Attempt the part corresponding to the number/position you signed the cover sheet. Thus you should attempt part (1) if you are the first signatory and so on. Please write your name by your answer.

   Consider a Rabin cryptosystem with primes $N = 370397$ with prime factors $p = 587$ and $q = 631$ and Redundancy scheme $A$. For a message $m$ with corresponding ciphertext $c$, the values $b_1, b_2 \in \{-1, 1\}$ are $b_1 = \left(\frac{m}{N}\right)$ and bit $b_2 = -1$ if $m < \frac{1}{2}N = 185198$ and 1 otherwise. Give the message $m$ corresponding to the ciphertext $c$ and redundancy values $b_1$ and $b_2$, calculate the message $m$.

   (1) $(c, b_1, b_2) = (79257, 1, -1)$
   (2) $(c, b_1, b_2) = (129665, 1, -1)$
   (3) $(c, b_1, b_2) = (92481, 1, 1)$
   (4) $(c, b_1, b_2) = (335342, -1, -1)$
   (5) $(c, b_1, b_2) = (156972, -1, -1)$
   (6) $(c, b_1, b_2) = (279284, 1, 1)$

**Questions 2-5 are to be attempted as joint effort (as before).**

2. Show that for a Rabin cryptosystem with modulus $N$, the message $m$ corresponding to a ciphertext $c$ can be uniquely identified from the ciphertext $c$, the Jacobi symbol $\left(\frac{m}{N}\right)$ and the value of the least significant bit of the message $m$.

3. Use the Miller-Rabin test with bases $a = 2$, $a = 3$ and $a = 5$ to demonstrate that 36713 is likely to be prime.

4. Use Fermat's Little Theorem to show that $N = 4\ 745\ 134\ 633$ is a composite integer without explicitly finding its factors

5. Use the ideas of the Quadratic Sieve to find the two prime factors of $N = 4\ 745\ 134\ 633$ by considering the squares modulo $N$ of the following integers.

$$\begin{array}{r} 691\ 550\ 798 \\ 3\ 574\ 574\ 857 \\ 4\ 356\ 453\ 643 \\ 2\ 353\ 454\ 165 \\ 1\ 875\ 501\ 478 \\ 2\ 232\ 107\ 551 \end{array}$$

# MT3660/4660/5466
# Cryptography II
# Group Work Teaching Week 5

9 February 2021

Each group will get a mark out of 2 based on engagement with the session.
It is not necessary to complete all questions to obtains a mark of 2.
Do **NOT** erase your whiteboard after the session is over.

**Change to Process**. The relevant part of Question 1 is to be attempted individually. A serious individual attempt has to be made to the relevant part in order for an individual to be awarded the overall group mark. Questions 2-4 are to be attempted as a joint effort (as in previous weeks).

Each online group should appoint one member to keep an MS Teams chat window open using the channel for your group. Do not use audio or video on MS Teams, as MS Teams is just there for the chat function. You can use MS Chat or email to summon the lecturer when you need help.

Make sure you are signed-in and that you have associated your account with Royal Holloway using the code WVTSJYJMBNQP. Check everyone has voice communication. Click "+" at bottom right to make new slides if needed.

1. **Individual**. Attempt the part corresponding to the number/position you signed the cover sheet. Thus you should attempt part (1) if you are the first signatory and so on. Please write your name by your answer.

   Consider textbook RSA cryptosystems with moduli $N_1 = 3233$, $N_2 = 7897$ and $N_3 = 8051$, where each cryptosystem has public key exponent $e = 3$. For a common message $m$, the ciphertexts encrypted under these three RSA cryptosystems are $c_i = m^e \bmod N_i$ $(i = 1, 2, 3)$. Given these three cipheretxts $(c_1, c_2, c_3)$ find the corresponding message $m$.

   (1) $(c_1, c_2, c_3) = (314, 5031, 1370)$
   (2) $(c_1, c_2, c_3) = (2631, 5281, 7354)$
   (3) $(c_1, c_2, c_3) = (1261, 3646, 3248)$
   (4) $(c_1, c_2, c_3) = (2676, 132, 5160)$
   (5) $(c_1, c_2, c_3) = (416, 2642, 5045)$
   (6) $(c_1, c_2, c_3) = (953, 3285, 2909)$

**Questions 2-5 are to be attempted as joint effort (as before).**

2. (a) If $p = 5 \bmod 6$ is prime and $a$ has a cube root modulo $p$, then show that either $a^{\frac{1}{6}(p+1)}$ or $-a^{\frac{1}{6}(p+1)}$ is a cube root of $a$ modulo $p$.

   (b) A Textbook RSA cryptosystem has modulus $N = 1\ 513\ 026\ 409$, where $N = pq$ is the product of two primes $p = 35573$ and $q = 42533$ satisfying $p, q = 5 \bmod 6$, and public key exponent $e = 3$. If the ciphertext $c = 604\ 452\ 931$ corresponding to message $m$ is received, then find this message $m$.
   HINT. Compute $m \bmod p$ and $m \bmod q$ and combine the results.

3. Consider a Textbook RSA cryptosystem with modulus $N = 34\ 582\ 693$ and public key exponent $e = 65\ 537$. If the private key exponent is $d = 24\ 570\ 993$, then find the factors of $N$.

4. Consider a Textbook RSA cryptosystem with modulus $N = 208903$ and public key exponent $e = 65537$, with a challenge ciphertext $c = 44869$. For a randomly generated $r = 195476$, a decryption Oracle $\mathcal{O}$ shows that the decryption of $c' = cr^e = 115181 \bmod 208903$ is 203221. Find the message $m$ corresponding to this challenge ciphertext $c = 44869$.

5. (a) Consider a Textbook RSA encryption process with modulus $N$ and public exponent $e = 3$. If message $m_1 = z + 1$ is encrypted to $c_1$ and the related message $m_2 = z - 1$ is encrypted to $c_2$, then show that $(16 + c_1 - c_2)z - 3(c_1 + c_2) = 0 \bmod N$.

   (b) If the modulus $N = 249559$ and ciphertexts $c_1 = 195190$ and $c_2 = 41973$ are received, then find the related messages $m_1 = z + 1$ and $m_2 = z - 1$.

**NOTE**. Q2(b) is a corrected version of the original, in which the primes $p$ and $q$ were omitted. These values were supplied during the session.
Q4 Typo in ciphertext corrected to $c = 44689$.

# MT3660/4660/5466
# Cryptography II
# Group Work Teaching Week 6

23 February 2021

Each group will get a mark out of 2 based on engagement with the session.
It is not necessary to complete all questions to obtains a mark of 2.
Do **NOT** erase your whiteboard after the session is over.

All questions to be attempted as joint work. There are no questions that have to be attempted individually in the Teaching Week 6 Group Work.

Each online group should appoint one member to keep an MS Teams chat window open using the channel for your group. Do not use audio or video on MS Teams, as MS Teams is just there for the chat function. You can use MS Chat or email to summon the lecturer when you need help.

Make sure you are signed-in and that you have associated your account with Royal Holloway using the code WVTSJYJMBNQP. Check everyone has voice communication. Click "+" at bottom right to make new slides if needed.

1. Consider the Problem DISCRETE-LOG-ADD specified below.

   Problem: DISCRETE-LOG-ADD.
   Input. Positive integer $n$ and $x, y \in \{0, \ldots, n-1\}$ with $\gcd(x, n) = 1$.
   Output. Integer $k$ $(0 \leq k < n)$ such that $[k]x = \underbrace{x + \ldots + x}_{k \text{ times}} = y \bmod n$.

   (a) Show that DISCRETE-LOG-ADD, that is to say a discrete logarithm problem in the finite cyclic group $(\mathbb{Z}_n, +)$ which is the additive group modulo $n$, can be solved in polynomial time.

   (b) Does the result of (a) have any direct relevance to the difficulty of the Discrete Logarithm Problem (DLP) in the finite cyclic group $\mathbb{F}_p^*$ ($p$ prime)?

2. Consider the solution of $17^x = 15 \bmod 599$, where 17 has order 299 modulo 599. Use the Silver-Pohlig-Hellman method to find $x$.

3. Consider the solution of $23^x = 59 \bmod 97$, where 23 is a primitive root modulo 97. Use the Baby-Step-Giant-Step method to find $x$.

4. Consider the solution of $3^x = 11 \bmod 31$, where 3 is a primitive root modulo 31. Use the Pollard Rho method to find $x$.

5. Consider the solution of $17^x = 192 \bmod 449$, where 17 is a primitive root modulo 449.

   (a) Find $17^{225} \bmod 449$ and find $17^{436} \bmod 449$.

   (b) If $x_2$ satisfies $17^{x_2} = 2 \bmod 449$ and $x_3$ satisfies $17^{x_3} = 3 \bmod 449$, then use the ideas of Index Calculus with Factor Base $\mathcal{B} = \{2, 3\}$ to show that

   $$\begin{pmatrix} 225 \\ 436 \end{pmatrix} = \begin{pmatrix} 4 & 3 \\ 3 & 2 \end{pmatrix} \begin{pmatrix} x_2 \\ x_3 \end{pmatrix} \quad \bmod 448.$$

   (c) Find $x_2$ and $x_3$ with $0 \leq x_2, x_3 < 448$.

   (d) Find $x$ such that $17^x = 192 \bmod 449$,.

# MT3660/4660/5466
# Cryptography II
# Group Work Teaching Week 7

2 March 2021

Each group will get a mark out of 2 based on engagement with the session. It is not necessary to complete all questions to obtains a mark of 2. Do **NOT** erase your whiteboard after the session is over.

All questions to be attempted as joint work. There are no questions that have to be attempted individually in the Teaching Week 6 Group Work.

Each online group should appoint one member to keep an MS Teams chat window open using the channel for your group. Do not use audio or video on MS Teams, as MS Teams is just there for the chat function. You can use MS Chat or email to summon the lecturer when you need help.

Make sure you are signed-in and that you have associated your account with Royal Holloway using the code WVTSJYJMBNQP. Check everyone has voice communication. Click "+" at bottom right to make new slides if needed.

1. **Diffie-Hellman**

   (a) What is the order of $g = 46$ in $\mathbb{F}_{149}^*$?

   (b) **Diffie-Hellman Problem (DHP)**.
   Given $(g, g^a, g^b) = (46, 39, 81)$, compute $g^{ab} \bmod 149$.

   (c) **Decisional Diffie-Hellman Problem (DDHP)**.
   Given $(g, g^a, g^b, g^c) = (46, 6, 81, 25)$, does $g^{ab}$ equal $g^c$ modulo 149?

2. **El Gamal Encryption**
   Consider an El Gamal encryption scheme with prime $p = 42\ 247\ 547$, base element $g = 2$ and public key $h = 17\ 272\ 111$. The message $m = 101$ is encrypted setting random value $k$ to $k_0$ (unknown) to give the ciphertext

   $$(c_1, c_2) = (g^{k0}, mh^{k0}) = (15\ 436\ 738,\ 21\ 770\ 117).$$

   A subsequent message $m'$ is encrypted setting the random value $k$ to $k_0 + 1$ (ie. simply incrementing previous value) to give the ciphertext

   $$(c_1', c_2') = (g^{k0+1}, m'h^{k0+1}) = (30\ 873\ 476,\ 18\ 896\ 988).$$

   What is the message $m'$?

3. **DSA-like Scheme** (Notation of Figure 17 of Notes p73)
Consider a DSA-like scheme with primes $q = 61$ and $p = 786\ 901$ with $p = 12\ 900q + 1$, in which the element $h = 123\ 456$ is chosen.

   (a) Find the element $g = h^{\frac{p-1}{q}} \bmod p$.

   (b) Alice has private signing key $x = 43$. What is Alice's public verification key $y$?

   (c) Alice signs the message $m$ with hash value $H(m) = 33$ using her secret signing key $x = 43$ and the random value $k = 19$. What is the signature $(r, s)$ generated by Alice?

   (d) Demonstrate that Verification process shows that the signature $(r, s)$ generated in part (c) is classified as "Valid".

4. **DSA Signature Verification Process**
Suppose $p$ and $q$ be odd primes such that $q$ divides $p - 1$. Suppose further that $h \in \{1, \ldots, p-1\}$ and that $g = h^{\frac{p-1}{q}} \bmod p$.

   (a) Show that the order of $g$ in $\mathbb{F}_p^*$ divides $q$.

   (b) If $m = n \bmod q$, then show that $g^m = g^n \bmod p$.

   (c) Show that a signature generated by the Digital Signature Algorithm (DSA) signature process is classified as "Valid" by the DSA verification process.

5. **DSA-like Scheme Forgery**
Consider the DSA-like scheme setup of Question 3, but in which Alice has public verification key $y = 189\ 881$.

   (a) Find Alice's private signing key $x$ using at most 25 modulo exponentiations. [Hint. Use a Baby-Step-Giant-Step approach.]

   (b) Forge a signature for a message $m$ with hash value $H(m) = 11$ that will be classified as "Valid" by Alice's public verification key.

   (c) Demonstrate this verification process.

# MT3660/4660/5466
# Cryptography II
# Group Work Teaching Week 8

9 March 2021

Each group will get a mark out of 2 based on engagement with the session. It is not necessary to complete all questions to obtains a mark of 2.
Do **NOT** erase your whiteboard after the session is over.

All questions to be attempted as joint work. There are no questions that have to be attempted individually in the Teaching Week 6 Group Work.

Each online group should appoint one member to keep an MS Teams chat window open using the channel for your group. Do not use audio or video on MS Teams, as MS Teams is just there for the chat function. You can use MS Chat or email to summon the lecturer when you need help.

Make sure you are signed-in and that you have associated your account with Royal Holloway using the code WVTSJYJMBNQP. Check everyone has voice communication. Click "+" at bottom right to make new slides if needed.

1. **Babai Rounding and Lattice Reduction**
   Consider a Closest Vector Problem (CVP) in the 2-dimensional lattice $\mathcal{L}$ generated by the basis vectors $b_1 = (25, 21)$ and $b_2 = (15, 14)$ with the target vector $w = (780857, 760560)$.

   (a) Find $\lambda_1, \lambda_2$ (as decimals) such that $w = \lambda_1 b_1 + \lambda_2 b_2$.

   (b) Use Babai rounding with this basis $\{b_1, b_2\}$ to find a lattice vector in $\mathcal{L}$ close to the target vector $w$.

   (c) Use a sequence of elementary row operations to reduce the lattice basis $\{b_1, b_2\}$ to a new basis $\{b'_1, b'_2\}$ for $\mathcal{L}$ with $|b'_1|, |b'_2| < 8$.

   (d) What is a shortest nonzero vector in this lattice $\mathcal{L}$?

   (e) What is the closest vector in the lattice $\mathcal{L}$ to the target vector $w = (780857, 760560)$?

   (f) Briefly explain why Babai rounding in part (b) with basis $\{b_1, b_2\}$ fails to find the closest lattice vector in $\mathcal{L}$ to the target vector $w$.

2. **Orthogonality Defect**

   The *Orthogonality Defect* of a basis $\mathcal{B} = \{b_1, \ldots, b_n\}$ of a lattice $\mathcal{L}$ is

$$\mathrm{OD}(\mathcal{B}) = \frac{\prod_{i=1}^{n} |b_i|}{\mathrm{Vol}(\mathcal{L})}.$$

   (a) Show that the Orthogonality Defect of a 2-dimensional lattice basis $\mathcal{B} = \{(p,q)(r,s)\}$ is $\mathrm{OD}(\mathcal{B}) = \dfrac{\sqrt{(p^2+q^2)(r^2+s^2)}}{|ps-qr|}$.

   (b) Show that $\mathrm{OD}(\mathcal{B}) \geq 1$ for a 2-dimensional lattice basis $\mathcal{B}$, with equality if and only if the lattice basis $\mathcal{B}$ is orthogonal.

   **Note**. $\mathrm{OD}(\mathcal{B}) \geq 1$ for a general $n$-dimensional lattice basis $\mathcal{B}$, with equality if and only if the lattice basis $\mathcal{B}$ is orthogonal.

3. **Closest Vector Problem (CVP) by Embedding**

   Consider a 6-dimensional lattice $\mathcal{L}$ with lattice basis matrix

$$B = \begin{pmatrix} 19 & 566 & 278 & 894 & 926 & 576 \\ 899 & 810 & 78 & 374 & 660 & 948 \\ 816 & 422 & 614 & 310 & 128 & 55 \\ 894 & 337 & 624 & 818 & 422 & 964 \\ 653 & 734 & 604 & 949 & 343 & 30 \\ 827 & 204 & 486 & 437 & 841 & 261 \end{pmatrix}.$$

   (a) What is the Orthogonality Deficit $\mathrm{OD}(B)$ (to 2 decimal places) of this basis $B$ for the lattice $\mathcal{L}$?

   (b) Find an LLL-reduced basis $B'$ of this lattice $\mathcal{L}$. What is the Orthogonality Deficit $\mathrm{OD}(B')$ (to 2 decimal places) of this reduced lattice basis $B'$ for the lattice $\mathcal{L}$

   (c) Use the embedding technique to find the closest vector in the lattice $\mathcal{L}$ to the target vector

$$w = (2624881, 1907601, 1697743, 2456604, 2258036, 2098212).$$

   **Note**. The Mathematica command `Norm[v]` gives the length of a vector $v$, so `Norm[B[[i]]]` gives the length of the $i^{\text{th}}$ row of a matrix $B$.

4. **Approximate Greatest Common Divisor Problem (AGCD)** Approximate multiples $X_0, \ldots, X_{n-1}$ of an unknown positive integer $p$ (bounded below by some integer $P$) are defined by

$$X_0 = pQ_0 + \epsilon_0, \ldots, X_{n-1} = pQ_{n-1} + \epsilon_{n-1},$$

where $Q_0, \ldots, Q_{n-1}$ are generated uniformly on $\{\mu - \alpha, \ldots, \mu + \alpha\}$ for integers $\mu > \alpha > 0$ and the errors $\epsilon_0, \ldots, \epsilon_{n-1}$ are generated uniformly on $\{-\beta, \ldots, \beta\}$ for a positive integer $\beta \ll \mu$.

The *Approximate Greatest Divisor Problem* (AGCD) is to determine the positive $p$ given the approximate multiples $X_0, \ldots, X_{n-1}$

Let $\mathcal{L}$ be the $n$-dimensional lattice arising from the AGCD problem with $n \times n$ basis matrix

$$B = \begin{pmatrix} 1 & -X_1 & -X_2 & \ldots & -X_{n-1} \\ 0 & X_0 & 0 & \ldots & 0 \\ 0 & 0 & X_0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & X_0 \end{pmatrix}.$$

(a) What is the volume of the lattice $\mathcal{L}$?

(b) Explain why $(Q_0, \ldots, Q_{n-1})B$ is likely to be the shortest vector the lattice $\mathcal{L}$ for large enough dimension $n$.

(c) Consider an AGCD Problem with $\mu = 300$, $\alpha = 100$, $\beta = 10$ and $P = 100$, in which $n = 6$ approximate multiples of $p$ are

$$(X_0, \ldots, X_5) = (113922, 78565, 115808, 62592, 73545, 85451).$$

Find a short vector in the lattice $\mathcal{L}$ for this AGCD Problem.

(d) Find the multipliers $(Q_0, \ldots, Q_5)$ for this AGCD Problem.

(e) Determine the Approximate Greatest Common Divisor $p$.

**Note**. The AGCD Problem can be used to construct a public key encryption cryptosystem.

# MT3660/4660/5466
# Cryptography II
# Group Work Teaching Week 9

16 March 2021

Each group will get a mark out of 2 based on engagement with the session. It is not necessary to complete all questions to obtains a mark of 2.
Do **NOT** erase your whiteboard after the session is over.

Each online group should appoint one member to keep an MS Teams chat window open using the channel for your group. Do not use audio or video on MS Teams, as MS Teams is just there for the chat function. You can use MS Chat or email to summon the lecturer when you need help.

Make sure you are signed-in and that you have associated your account with Royal Holloway using the code WVTSJYJMBNQP. Check everyone has voice communication. Click "+" at bottom right to make new slides if needed.

1. **GGH Encryption and Decryption**
   A GGH cryptosystem has private key lattice basis matrix $B$ and unimodular matrix $U$ given by

$$B = \begin{pmatrix} 13 & 2 & 1 & -2 \\ 2 & 29 & -3 & 1 \\ -2 & 3 & 53 & 3 \\ 4 & -2 & -3 & 79 \end{pmatrix} \quad \text{and} \quad U = \begin{pmatrix} 1 & 3 & 2 & -4 \\ 1 & 4 & 1 & 0 \\ -1 & -1 & -3 & 9 \\ -5 & -17 & -13 & 28 \end{pmatrix}.$$

   (a) Find the public key lattice basis matrix $B'$.

   (b) Encrypt the message $(-5, 2, 3, 5)$ using the error vector $(2, 1, -2, 3)$.

   (c) Decrypt the ciphertext $396, -3834, -5356, 16906)$.

2. **GGH Cryptanalysis**
   A GGH cryptosystem has public key lattice basis matrix $B'$ given by

$$B' = \begin{pmatrix} -8 & 199 & -34 & -190 & 154 & -189 \\ 42 & -345 & 150 & 568 & -462 & 613 \\ -135 & 181 & -330 & -1330 & 1035 & -1215 \\ 125 & -360 & 669 & 1161 & -931 & 2230 \\ 132 & 624 & 62 & 969 & -602 & 197 \\ 15 & -1020 & -222 & 779 & -1039 & -747 \end{pmatrix}.$$

   Decrypt the ciphertext $(621, -2095, 1727, 6490, -5970, 5183)$.

3. **GGH Special Form Private Key**

   Consider a GGH cryptosystem of dimension 3 with an integer diagonal public key 3×3 lattice basis matrix $B$ and integer lower triangular unimodular 3×3 matrix $U$ (so $U_{ij} = 0$ if $j > i$).

   (a) Show that the public key 3×3 lattice basis matrix $B'$ is a lower triangular matrix.

   (b) Find an orthogonal 3×3 lattice basis matrix $B^*$ and corresponding unimodular matrix $U^*$, expressed in terms of the elements of $B'$, with $B = U^* B^*$.

   (c) In such a GGH cryptosystem with public key basis matrix

$$B' = \begin{pmatrix} 7 & 0 & 0 \\ 35 & 11 & 0 \\ 21 & -44 & -17 \end{pmatrix},$$

   decrypt the ciphertext $(393, -242, -121)$.

4. **LWE Problem and Cryptosystem**

   Consider an LWE Problem based on $b = As + e \bmod 89$, where

$$A = \begin{pmatrix} 64 & 13 \\ 13 & 3 \\ 43 & 33 \\ 29 & 82 \\ 35 & 66 \end{pmatrix} \quad \text{and} \quad b = \begin{pmatrix} 24 \\ 18 \\ 37 \\ 46 \\ 82 \end{pmatrix}.$$

   (a) Find the secret $s = (s_1, s_2)^T$ in this LWE Problem.

   (b) Consider a LWE cryptosystem modulo 89 with public key $(A, b)$. Find the ciphertext parts $v$ and $w$ obtained by encrypting the message $\theta = 1$ using the binary vector $(1, 0, 1, 0, 1)$.

   (c) Consider a LWE cryptosystem modulo 89 with public key $(A, b)$. Find the message bit $\theta$ obtained by decrypting the ciphertext parts $v = (42, 85)$ and $w = 19$.

5. **LWE Small Secret**

The Learning with Errors (LWE) Problem is based on $b = As{+}e \bmod q$, where $s \in \mathbb{F}_q^n$ is the secret, $A$ is an $m \times n$ matrix with entries uniformly distributed on $\mathbb{F}_q$ and error vector $e$ with components $e_1, \ldots, e_m \sim \chi$, where his error distribution $\chi$ on $\mathbb{F}_q$ is concentrated about 0.

The expression $b = As{+}e$ can be partitioned into the first $n$ components and the remaining $m - n$ components to give

$$\left(\frac{b_0}{b_1}\right) = \left(\frac{A_0}{A_1}\right) s + \left(\frac{e_0}{e_1}\right) \quad \bmod q,$$

where $A_0$ is an $n \times n$ matrix and $A_1$ is an $(m-n) \times n$ matrix and so on. Suppose that $A_0$ is an invertible $n \times n$ matrix modulo $q$ and consider the $(m - n) \times m$ matrix

$$P = \left( \, -A_1 A_0^{-1} \, \middle| \, I_{m-n} \, \right).$$

By applying $P$ to the above expression, construct an LWE Problem based on $b' = A's' + e' \bmod q$ where $A'$ is an $(m-n) \times n$ matrix and so on, and in which the components $e'_1, \ldots, e'_{m-n}$ of $e'$ and the components $s'_1, \ldots s'_n$ of $s'$ all have the concentrated distribution $\chi$.

# MT3660/4660/5466
# Cryptography II
# Group Work Teaching Week 10

23 March 2021

Each group will get a mark out of 2 based on engagement with the session. It is not necessary to complete all questions to obtains a mark of 2.
Do **NOT** erase your whiteboard after the session is over.

Each online group should appoint one member to keep an MS Teams chat window open using the channel for your group. Do not use audio or video on MS Teams, as MS Teams is just there for the chat function. You can use MS Chat or email to summon the lecturer when you need help.

Make sure you are signed-in and that you have associated your account with Royal Holloway using the code WVTSJYJMBNQP. Check everyone has voice communication. Click "+" at bottom right to make new slides if needed.

**Note**. You may assume that the *isomorphism class* of an elliptic curve group $E(\mathbb{F}_p)$ is either a cyclic group $C_m$ or product of two cyclic groups $C_m \times C_n$ with $n \geq 2$ dividing $m$.

**Note**. The Elliptic Curve Tool at `https://graui.de/code/elliptic2/` should be used for elliptic curve calculations. In particular, the successive multiples of a point can be found by clicking on that point in the graph. You may use any clearly stated result obtained from this Elliptic Curve Tool.

1. **Elliptic Curve Elements of Order 2**
   Consider the elliptic curve group $E(\mathbb{F}_p)$: $y^2 = x^3 + ax + b$, where the discriminant $4a^3 + 27b^2 \neq 0 \bmod p$.

   (a) Show that an elliptic curve point $(x, y) \in E(\mathbb{F}_p)$ has order 2 if and only if $y = 0$.

   (b) Show that $E(\mathbb{F}_p)$ has at most three elements of order 2.

   (c) Show that $E(\mathbb{F}_p)$ cannot have exactly two elements of order 2.

   (d) If $E(\mathbb{F}_p)$ has three elements of order 2, then show that the isomorphism class of $E(\mathbb{F}_p)$ is $C_m \times C_n$ for some $m, n$ with $n \geq 2$ dividing $m$.

2. **Elliptic Curve Isomorphism Classes**.

   (a) By considering the order of the group, determine the isomorphism class of the elliptic curve group $E(\mathbb{F}_{31})\colon y^2 = x^3 + x + 3$.

   (b) By considering the order of the group, determine the isomorphism class of the elliptic curve group $E(\mathbb{F}_{31})\colon y^2 = x^3 + 2x + 4$.

   (c) By considering the order of the group and the number of elements of order 2, determine the isomorphism class of the elliptic curve group $E(\mathbb{F}_{31})\colon y^2 = x^3 + 16x + 17$.

   (d) By considering the order of the group and the number of elements of order 2, determine the isomorphism class of the elliptic curve group $E(\mathbb{F}_{31})\colon y^2 = x^3 + 28x + 13$.

3. **Elliptic Curve Diffie-Hellman Key Agreement**
   Consider an elliptic curve Diffie-Hellman key agreement scheme in the elliptic curve group $E(\mathbb{F}_{53})\colon y^2 = x^3 + 2x + 1$ with base point $(0, 1)$. Alice has secret integer $z_A$ and public point $Q_A = [z_A](0, 1) = (7, 26)$. Bob has secret integer $z_B$ and public point $Q_B = [z_B](0, 1) = (39, 12)$.

   (a) What is the order of the elliptic curve group $E(\mathbb{F}_{53})$?

   (b) What is the order of the base point $(0, 1)$?

   (c) Find Alice's secret integer $z_A$.

   (d) Find Alice and Bob's shared secret point $K = [z_A z_B](0, 1)$.

4. **Elliptic Curve Discrete Logarithm (SPH Method)**
   Consider an elliptic curve discrete logarithm problem in the elliptic curve group $E(\mathbb{F}_{73})\colon y^2 = x^3 + 7x + 1$ given by

   $$[\lambda]\ (0, 1) = (1, 3),$$

   where the base point $(0, 1)$ has order 77.

   (a) Find $[11](0, 1)$, $[11](1, 3)$ and the subgroup $\langle [11](0, 1)\rangle$.

   (b) Find $[7](0, 1)$, $[7](1, 3)$ and the subgroup $\langle [7](0, 1)\rangle$.

   (c) Find the value of $\lambda$ modulo 7 and the value of $\lambda$ modulo 11.

   (d) Use the Chinese Remainder Theorem to find the elliptic curve discrete logarithm $\lambda$ satisfying $[\lambda](0, 1) = (1, 3)$ in $E(\mathbb{F}_{73})$.