Cryptology - Week 3 worksheet

These exercises are to consolidate the lecture material from week 3. In this worksheet, you will practice Euclid's algorithm, Sun-Tzu's theorem and Diffie-Hellman.

- Question 1 is to get practise with Euclid's corollary and Sun-Tzu's remainder theorem.
- Question 2 is to get improve your understanding of Diffie-Hellman and the algorithms that go into running Diffie-Hellman. A version of this question is an option for an exam question (both for the major and the minor).
- Question 3 is to introduce to ElGamal encryption, which we will cover in the lecture in week 4.
- Question 4 is an optional question to see how we might construct Diffie-Hellman-style key exchanges which cannot be broken by Shor's quantum algorithm.

1. (a) Using Euclid's algorithm, find the greatest common divisor (gcd) d of 754 and 512.

   (b) Following the method in the proof of Euclid's corollary, find integers a and b such that $754a + 512b = d$.

   (c) Using Sun-Tzu's Remainder Theorem, find $x \pmod{17 \cdot 11}$ such that $x \equiv 5 \pmod{17}$ and $x \equiv 2 \pmod{11}$.

2. **A version of this question is an option for an exam question.**

   (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 g for the group $(\mathbb{Z}/11\mathbb{Z})^*$ under operation $* = \times \pmod{11}$. Justify your answer.

   (c) Using Euclid's corollary, find the inverse of the g that you found in (b) in $(\mathbb{Z}/11\mathbb{Z})^*$.

   (d) Using your public parameters $(p, g) = (11, g)$, Hellman sends you his public key $g^h = 7$. Your secret key is $d = 6$. Compute your shared secret with Hellman.

(e) Prove that Hellman's secret $\mathrm{sk_H} = h$ is only defined mod 10, i.e., that you could imitate Hellman using any secret key of the form $\mathrm{sk_H} + 10n$, for $n \in \mathbb{Z}$.
Hint: Use Fermat's Little Theorem.

(f) Using Sun-Tzu's Remainder Theorem to compute discrete logarithms, compute Hellman's secret (mod 10).

3. (El Gamal Encryption in disguise)

In this question, we'll introduce El Gamal's encryption algorithm, that extends Diffie-Hellman's key exchange algorithm. We'll work in $\mathbb{Z}/11\mathbb{Z}$, with a generator 2. You are given Alex's public key value $pk_A = 5$.

Firstly, let's encrypt:

(a) Pick the message that you'd like to send to Alex. It must be in $(\mathbb{Z}/11\mathbb{Z})^*$. Call it m.

(b) Pick your secret $h \in \{1, 2, \ldots, 10\}$ and compute your public key 2^h (mod 11).

(c) Calculate your shared secret with Alex $ss = pk_A^h$.

(d) Calculate the ciphertext $c = m \cdot ss$.

(e) Why must $m \neq 0$?

A ciphertext is somewhat useless if it can't be decrypted (knowing the secret key)

(f) Calculate Alex's private key (and explain why doing so doesn't break Diffie-Hellman security).

(g) Recover m.
Hint: you may want to work algebraically first.

(h) Why is this a good method for encryption?

4. (Optional) 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).