4400-001 - SPRING 2022 - WEEK 6 (2/15, 2/17)
DIFFIE-HELLMAN AND RSA

Some of these exercises can be found in Savin - Chapter 10.

Exercise 1 (required). Computing powers and finding primitive roots. Let $\mathbb{K}$ be a finite field (i.e. a field with only finitely many elements). A *primitive* root $g \in \mathbb{K}^\times$ is an element such that

$$\mathbb{K}^\times = \{g^0, g^1, g^2, \dots\}$$

i.e. every non-zero element in $\mathbb{K}$ can be written as a power of g.
Fact: $g \in \mathbb{K}^\times$ is a primitive root if and only if $g^d \neq 1$ for any proper divisor d of $|\mathbb{K}^\times|$.

(1) Use the method of successive squaring to compute

$$5^{143} \mod 1979$$
$$2^{143} \mod 1979$$

(2) For each of the following primes, find the smallest positive integer k such that k is a primitive root modulo p (i.e. in $\mathbb{F}_p$): 13, 31, 47, 41.

(3) Find a primitive root in $\mathbb{Z}[i]/(3)$.

(4) Find a primitive root in $\mathbb{F}_2[x]/(x^4 + x + 1)$ (you may use without assumption that $x^4 + x + 1$ is irreducible/prime in $\mathbb{F}_2[x]$, so that this is a field).

Exercise 2.

(1) Find a partner, and then establish a secret shift cypher key via Diffie-Hellman with $g = 7$ and $p = 71$. Use this cypher to exchange the names of your favorite animals.

(2) Choose a public RSA key, then find a partner. Transmit to your partner the message "ALOHA" or "MAHALO" using their public key. Decode their message to you. Here we use the following encoding of (a subset of) the Hawaiian alphabet (see also p.138 of Savin):

E	A	O	H	L	M	N	K	I
1	2	3	4	5	6	7	8	9

Exercise 3 (required). Decrypting and encrypting.

(1) A shift cypher key is established using the Diffie-Hellman method with $g = 5$ and $p = 47$. The numbers exchanged were $X = 38$ and $Y = 3$. Find the key, then use it to decipher

EQPITCVWNCVKQPU

(2) Encypt KO-NA using the RSA cypher with $m = 1517$ and $e = 7$ and the encoding of the partial Hawaiian alphabet from Exercise 2.

(3) Using the RSA cypher with $m = 1517 = 37 \cdot 41$ and $e = 11$, decipher the message:

1373 1149 108

using the encoding of the partial Hawaiian alphabet from Exercise 2.

(4) (*Bonus for 6 points; not required*). My RSA public key is $m = 39597$, $e = 5$. In the following, use the encoding of the partial Hawaiian alphabet from Exercise 2.

(a) Use my RSA key to encrypt the message "AHA" for me to read.

(b) Suppose your RSA public key is $m = 208 = 11 \cdot 19$ and $e = 7$. Add the digital signature "MOANA" to your message (this does not mean just encode "MOANA" using my key! See the Digital Signatures paragraph on p. 141 of Savin).

(c) I made a dangerous choice for my public key! Crack it (i.e. factor m) using the factorization method described in Week 2, Exercise 5.

Exercise 4. Some well-adapted encodings.

(1) Working with a partner, construct a field $\mathbb{F}_{27}$ with 27 elements, and match the elements up with the 26 letters of the English alphabet, leaving one element to mean "space." This encoding is nicely adapted to transmitting messages in English! Find a primitive root in $\mathbb{F}_{27}$ and run Diffie-Hellman in $\mathbb{F}_{27}$ to send some messages this way.

(2) Computers store data in binary as strings of zeroes and ones. A byte is a string of 8 zeroes or 1s. Can you construct a field whose elements naturally encode bytes? What would you need to do to run Diffie-Hellman in this field?

(3) In practice these two methods would not work well because a computer could easily reverse-engineer the key from the public data with such small fields. How, in principal, could you make a version of (1) and (2) that was more secure against decryption? Remember that normally we need to send a lot more than a single letter or a single byte!