Homework 27 Solutions

Problems

1. **Alice and Bob want to securely communicate over an unsecure line. They use the following scheme to convert a message into numbers (and vice versa): each letter corresponds to a number mod $N = 143$ in the following way:**

A	B	C	D	E	F	G	H	I	J	K	L	M
34	2	106	17	10	119	16	37	68	102	76	82	92

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
7	12	109	47	101	63	30	69	45	133	80	128	89

Alice tells Bob that, after having translated his message into a sequence of numbers, he should then raise each of them to the 103rd power (reduced mod 143). One day, Alice receives the following message from Bob:

$$21, 122, 140, 17, 2, 24, 67, 122, 140.$$

Let's try to decode it!

(a) **We know that the first letter in the message corresponds to some number x. Because of the way that Bob used to encode the message, We know that $x^{103} \equiv 21 \pmod{143}$. Solve this for x!**

(b) **This should give you the first letter in the message. What is it?**

(c) **Now decode the rest of the message!**

Let's run through how we do the first letter:

If $x^{103} \equiv 21 \pmod{143}$ then x is just going to be the 103rd root of 21 modulo 143. Now $143 = 11 \times 13$ so that $\phi(143) = 120$. Next we compute that $1/103 = 7 \pmod{120}$ (using the Euclidean Algorithm backwards). So we see that $21^{1/103} = 21^7 \pmod{143}$. We compute, using doubling, that this is $\boxed{109} \pmod{143}$, which is the number corresponding to P.

Only the last step of this needs to be done separately for each letter. The message turns out to be *PARTY CZAR* — we shall leave it to you to decide which of the 3 of us this is.

2. (a) **Alice wishes to send a secret message to Bob using the public-key cryptographic protocol discussed in today's lecture (and in Chapter 22 of the book). Upon request, Bob sends her $n = 143$ and $k = 17$. If Alice wants to transmit the encrypted version of the message $m = 24$, what should she send Bob?**

Alice should send $24^{17} \equiv \boxed{7} \pmod{143}$ to Bob (she can compute this using the doubling method).

(b) **Later, Ann wants to communicate with Bob. Bob chooses $p = 11$, $q = 17$, $k = 23$. After sending Ann $n = 187$ and $k = 23$, he receives from her the number 177. What was Ann's message?**

Ann wanted to send the message x, so she sent Bob $x^{23} = 177 \pmod{187}$. To decode this Bob wants to compute $177^{1/23} \pmod{187}$. Now, $\phi(187) = 10 \times 16 = 160$ and Bob computes that $1/23 = 7 \pmod{160}$. So $x = 177^{1/23} = 177^7 = (-10)^7 \pmod{187}$ and Bob computes this to be $\boxed{12}$.

(c) **Eve listens in on a communication between Bob and Amanda. She knows that Bob transmitted to Amanda $n = 2047$, $k = 125$. Amanda responded with the number 2. What was Amanda's message? (Computational hint:** $2^{11} = 2048 = 1 \pmod{2047}$**. Use this to your advantage.)**

Our first step is to factor 2047. Since the only way we know of to factor is trial division, we check 2, then 3, then 5, then... We eventually find that

$$2047 = 23 \cdot 89.$$

Thus

$$\phi(2047) = 22 \cdot 88.$$

So in order to decode the message 2, we need to compute

$$2^{1/125} \pmod{2047}.$$

The first step toward computing this root is finding

$$1/125 \pmod{\phi(2047)},$$

which we do using Euclid's algorithm. We find that

$$1/125 \equiv 1301 \pmod{1936}.$$

Thus

$$2^{1/125} \equiv 2^{1301} \pmod{2047}.$$

We now use the computational hint. Since $1301 = 11 \cdot 118 + 3$, we have

$$2^{1301} = 2^{11 \cdot 118 + 3} = (2^{11})^{118} \cdot 2^3 \equiv 1^{118} \cdot 2^3 = 8 \pmod{2047}.$$

So the initial message was $\boxed{8}$.

Note that in this case, since the order of 2 is so small, there is a way to break this message without factoring 2047 (this would be useful if 2047 were large enough that it was truly difficult to factor). Since the 125th root of 2 must be a power of 2, and there are only 10 powers of 2 that aren't 1, we can just check all of their 125th powers.

$$\begin{aligned}
2^{125} &\equiv 2^4 = 16 \neq 2 \pmod{2047} \\
4^{125} &\equiv 2^8 = 256 \neq 2 \pmod{2047} \\
8^{125} &\equiv 2^{12} \equiv 2 \pmod{2047}
\end{aligned}$$

and we are done.

This is not a problem in the real world, since in practice there are only a few numbers with such small orders, and even if you receive a message that happens to be one of them, you wouldn't know to check that it had small order.