Homework 26 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 6 of us this is.

2. **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).

3. **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 $\boxed{12}$.