Lab Project for August 1, 2012

Forging a Digital Signature

This problem has you forge a digital signature. We're going to use RSA, probably the most common public key crypto system used in the Web. You don't need to know why what follows works, too — you just need to know how.

RSA, like Rabin, uses modular arithmetic. You have a public key (e, n) and a private key d. To *sign* a message m, compute:

$$m_s = m^d \bmod n$$

Then the signature and the message are sent to the recipient. To validate the signature, she computes:

$$m' = m_s^e \bmod n$$

and compares m' to m. If they are the same, the message has not been altered, and it was sent by the person who has the associated public key (e, n).

Or so goes the theory. As mentioned in class, you need to be *very, very careful* with cryptographic protocols such as digital signatures. Let's explore this a bit more.

Alice and Bob have the following public and private keys:

$n_{\text{Alice}} = 95$, $e_{\text{Alice}} = 59$, $d_{\text{Alice}} = 11$
$n_{\text{Bob}} = 77$, $e_{\text{Bob}} = 53$, $d_{\text{Bob}} = 17$

Suppose Alice wants Bob to sign a contract. There are 26 possible contracts, labeled A (0) to Z (25) (see Figure 1). She wants Bob to sign contract I, but he refuses. So she has him sign contract F:

$$5^{17} \bmod 77 = 3$$

Later on she convinces him to sign contract R:

$$17^{17} \bmod 77 = 19$$

Alice then multiple the two values for the contracts together and reduces them mod77. She does the same for the signatures:

$$5 \times 17 \bmod 77 = 8$$

$$3 \times 19 \bmod 77 = 57$$

Now Alice goes to Judge Janice, and says that Bob signed contract I (8). As proof she gives the signature, 57. Judge Janice validates the signature as follows:

$$57^{53} \bmod 77 = 8$$

What You Are To Do

Naturally, Bob isn't going to take this lying down! So he has Alice sign 2 other contracts. Then he goes back to Judge Janice, saying that Alice signed contract U, with signature 20. Alice denies this. Judge Janice computes:

$$20^{59} \bmod 95 = 20$$

What two contracts did Bob have Alice sign, in order to pull off this attack?

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Figure 1: Representing letters as numbers