Sheet2

Link to calculator for modular exponentiation: `tinyurl.com/Master04`.
Link to calculator for modular inverses: `tinyurl.com/Master05`.
List of a few primes:

Number	100	1000	10000	100000	1000000
Next	101	1009	10007	100003	1000003
Previous	97	997	9973	99991	999983

Questions 4 onwards are to be done in pairs — A and B.

1. Work out $7^5 \pmod{11}$. Do this yourself: $7^{=}49 \equiv 5 \pmod{11}$, so $7^5 = 7^{2+2+1} \equiv 5 * 5 * 7 \cdots$. Check your answer with the calculator.
2. Work out $23^{29} \pmod{97}$ using the calculator.
3. Diffie-Hellman Key Exchange.
   Suppose that A and B agree the prime 11 (in practice, they would choose a far larger number), and the base 2. A chooses 3 and B chooses 7 (both have no common factor with $p - 1 = 10$). What does A send to B? What does B send to A? What shared secret do they end up with?
4. Diffie-Hellman Key Exchange.
   Choose a prime p (I suggest two digits*) between you (note that this *isn't* a secret!)), and a base g (say 2, also not a secret). A and B then choose a private number each (a and b: these *are* the secrets). A computes $g^a \pmod{p}$ and tells this to B. Simultaneously, B computes $g^b \pmod{p}$ and tells this to A. Then A raises the message from B to the power $a \pmod{p}$ and B raises the message from A to the power $b \pmod{p}$. A and B then check that they have the same number, which could be used as the key of a code.
5. Repeat with a larger prime from the table above.
6. Diffie-Hellman Message Passing.
   Choose a prime p (I suggest two digits, but bigger than 26) between you, and a base g (say 2). A and B then choose a private number each (a and b). A then chooses secretly a letter (call it L), and encodes as ($a = 1$, $b = 2$, $c = 3$, $\ldots$). A sends $L^a \pmod{p}$ to B. B raises this to the power $b \pmod{p}$ and sends this to A. A in the meantime has computed a', the inverse of $a \pmod{p}$, and raises B's message to this power, modulo p. B in the meantime has computed b', the inverse of $b \pmod{p}$, and raises A's message to this power, modulo p. B should now have the letter L that A sent.
7. Repeat with a larger prime from the table above.

* 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.