JUNE 15TH MATH PROBLEM SET

Lots of people working in cryptography have no deep concern with real application issues. They are trying to discover things clever enough to write papers about. – Whitfield Diffie

1. Choose a moderately large prime, n. Then find a generator x. Write them publicly on a chalk board. Choose your own secret key a (make it big also), compute

$$x^a (\text{mod } p)$$

and write it on the chalkboard too. This makes up your public key.

2. Make a message, m. This should be a sequence of numbers less than your prime. Keep it short but meaningful.

3. Find a neighboring country and identify their public key $(n', x', x'^{a'})$. Choose b' and write for them on the chalkboard $x^{b'} (\text{mod } n)$ and $m \cdot (x^{a'})^{b'} (\text{mod } n)$. See if they can decrypt your message. Have them do the same for you (points may be available). Note to decrypt, compute the inverse of $x^{ab} (\text{mod } n)$ and multiply it by the message they send you, mod n.

This is called ElGamal public key encryption.