ElGamal

----- Motivation ---

The ElGamal encryption system is an asymmetric key encryption algorithm for public key cryptography which is based on the Diffie-Hellman key exchange. The advantage of the ElGamal algorithm is the generation of keys using discrete logarithms.

ElGamalhas the disadvantage that the ciphertext is twice as long as the plaintext and it has the advantage that the same plaintext gives a different ciphertext (with near certainty) each time it is encrypted.

ElGamal encryption is used in the free GNU privacy guard software, recent versions of PGP, and other cryptosystems.

----- Method---

-- Encrypt --

Step 1: Public Parameter Creation

A trusted party must choose and publish a (large) prime p, and an element g modulo p of large (prime) order. (attach popup 3)

Bob's part: Key Creation Step 2: choosing a private key

Bob has to choose a private key 1≤ a ≤ p-1.

Step 3: Compute the public key and publishing it

Bob computes A = $g^a mod(p)$ and publishes it.

Now, we get to Encryption (What Alice does): Step 4: Choose plaintext m and a random ephemeral key k

The number k is called an *ephemeral key*, since it exists only for the purposes of encrypting a single

Message. So, ALice will pick a random number for the secret key and pick a message to encrypt.

Step 5: Compute $c_1 and\ c_2$

Use Bob's public key A, to compute:

$c_1 = g^k\ (mod\ p)$

$c_2 = mA^k\ (mod\ p)$

Step 6: send ciphertext!

Send ciphertext ($c_1,\ c_2$) to Bob.

-- Decrypt --

Recall, Bob knows the values of a and A. And has received the cipher text $(c_1,\ c_2)$ from Alice. Bob

only has to do one simple step:

Compute $(c_1^a)^{-1} * c_2\ (mod\ p)$. This quantity is equal to m.

----- Example ---

-- Encrypt --

Step 1: Public Parameter Creation

For our example, let's use: p = 2579 and g = 2

Bob's part: Key Creation Step 2: choosing a private key
Let's use a = 765

Step 3: Compute the public key and publishing it
Bob computes A = $g^{a} mod(p) = 2^{765}\ mod\ 2579 = 949$

Now, we get to Encryption (What Alice does): Step 4: Choose plaintext m and a random ephemeral key k
let's use m = 1299 and random key k = 853

Step 5: Compute $c_1 and\ c_2$
In our example, $c_1 = 2^{853}\ mod\ 2579 = 435\ mod\ 2579$ and
$c_2 = 1299\ (949)^{853}\ mod\ 2570 = 2396\ mod\ 2579$

Step 6: send ciphertext!
So, Alice would send (435, 2396) to Bob.

-- Decrypt ---
In our example, Bob will compute: $m' = (2579^{765})^{-1} * 2396\ \ mod\ 2579 = 1299\ mod\ 2579$