El Gamal Public Key Cryptosystem

Directly based on the discrete log problem.

One interesting thing: one plaintext can map to different ciphertexts, but all of those different ciphertexts map back to the original plaintext. Thus, the ciphertext is "bigger" than the plaintext. (Specifically, the ciphertext is twice as many bits.)

In some sense, El Gamal is slower than RSA because it had "extra ciphertext" so to speak.

Public Keys
Prime number: q
Generator/Primitive Root: $\alpha < q$.

Alice Creates Privately
She selects a private key, $1 < X_A < q - 1$
Calculate $Y_A = \alpha^{XA} \bmod q$

Last Public Key: Y_A (so the full set is $\{q, \alpha, Y_A\}$

How to Send a Message to Alice
We are Bob and we want to send Alice a message, M ($1 < M < q$)
Bob picks a random integer, *k*, $k < q$.
Bob calculates $K = (Y_A)^k \bmod q$ (This is really $\alpha^{XA*k} \bmod q$)

$C_1 = \alpha^k \bmod q$
$C_2 = KM \bmod q$

So, Bob sends to Alice (C_1, C_2)

How Alice Decrypts
Alice receives

$C_1 = \alpha^k \bmod q$
$C_2 = KM \bmod q$

Big Picture, Alice needs to determine $K^{-1} \bmod q$.

1. Alice calculates $K = (Y_A)^k = \alpha^{XA*k} \bmod q = (\alpha^k)^{XA} = (C_1)^{XA} \bmod q$.
2. Alice calculates $K^{-1} \bmod q$ via the Extended Euclidean.
3. Alice recovers M by calculating $K^{-1}C_2 = (K^{-1}KM) = M \bmod q$.

Example by Hand
$q = 13$, $\alpha = 2$

Alice selects $X_A = 4$, so $Y_A = 2^4 = 3 \bmod 13$

Bob's message is M = 8.

Bob selects

k = 8, $C_1 = 2^8 = 9 \bmod 13$, $K = 3^8 = 9 \bmod 13$, $C_2 = KM = 9*8 = 7 \bmod 13$
k = 10, $C_1 = 2^{10} = 10 \bmod 13$, $K = 3^{10} = 3 \bmod 13$, $C_2 = KM = 3*8 = 11 \bmod 13$

In one instance, Alice receives (9, 7).
In another instance, Alice receives (10, 11).

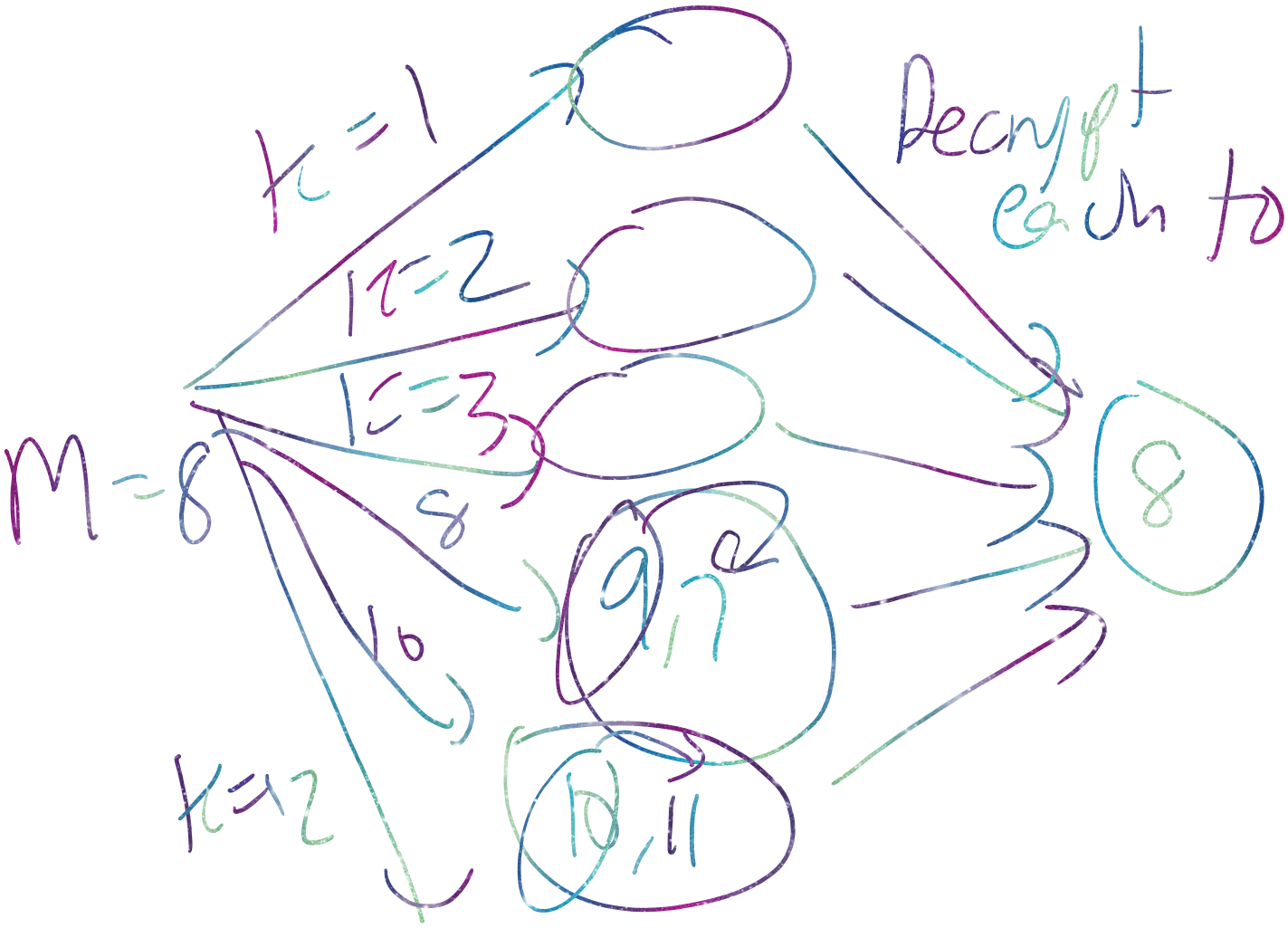
In the first instance, when Alice receives (9, 7), she calculates $C_1^{XA} = 9^4 = 9 \bmod 13$. (So Alice has recovered K, which we see is correct.)

Alice calculates $9^{-1} \bmod 13$ via the Extended Euclidean Algorithm. $9^{-1} = 3 \pmod{13}$.
Alice takes $K^{-1}C_2 = 3*7 = 21 = 8 \bmod 13$ (which is indeed M).

In the second instance, when Alice receives (10, 11), she calculates calculates$10^4 = 3 \bmod 13$. (So Alice has recovered K, which we see is correct.)
Alice calculates $3^{-1} \bmod 13$ via the Extended Euclidean Algorithm, $3^{-1} = 9 \pmod{13}$
Alice takes $K^{-1}C_2 = 9(11) = 99 = 8 \pmod{13}$ (which is M)

El Gamal Picture

Monday, November 2, 2020 12:01 PM



each block has $q-1$ possible encryptions.