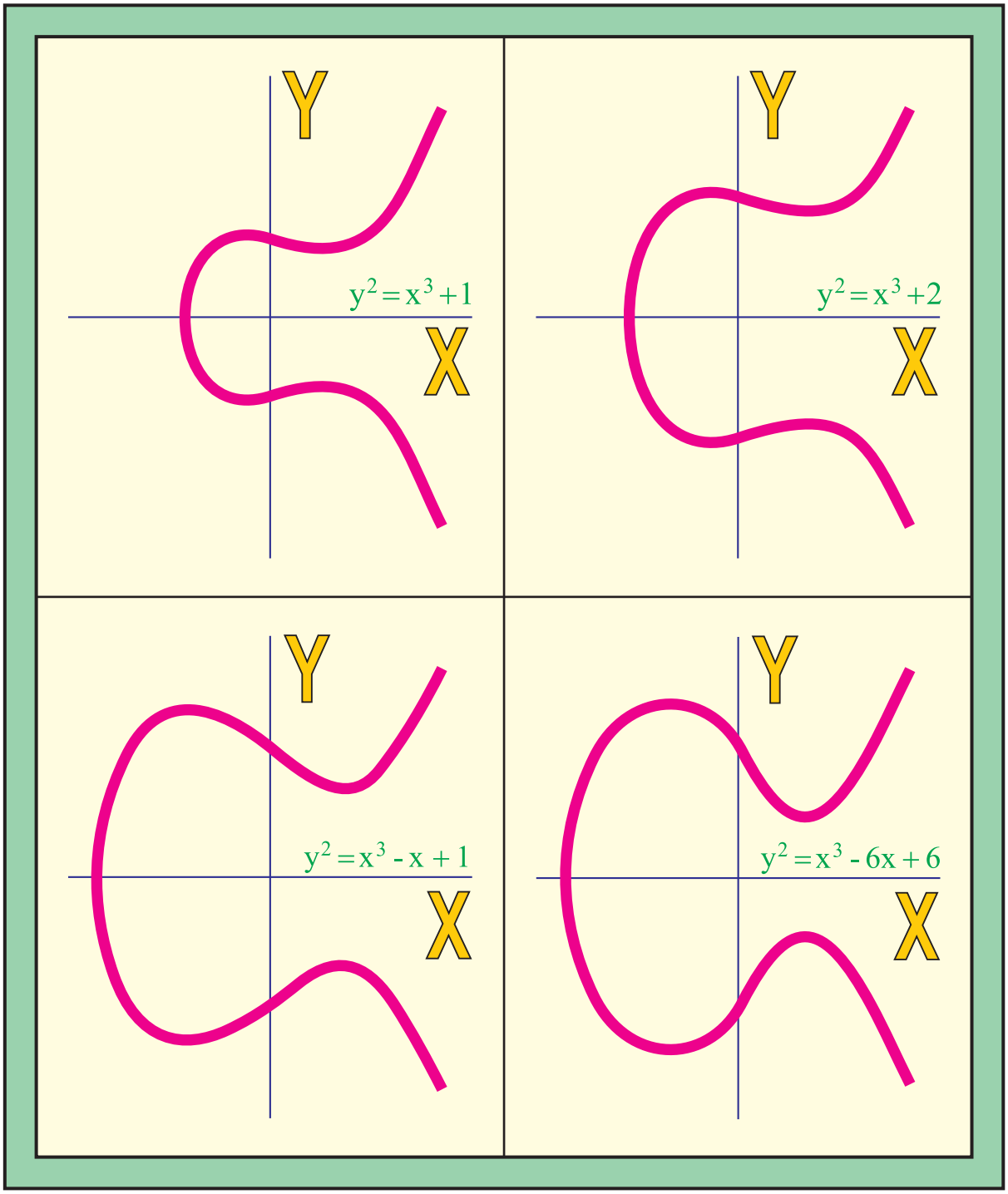
CURVA ELÍPTICA

Criptografia ECDH



Elliptic Curve Diffie - Hellman

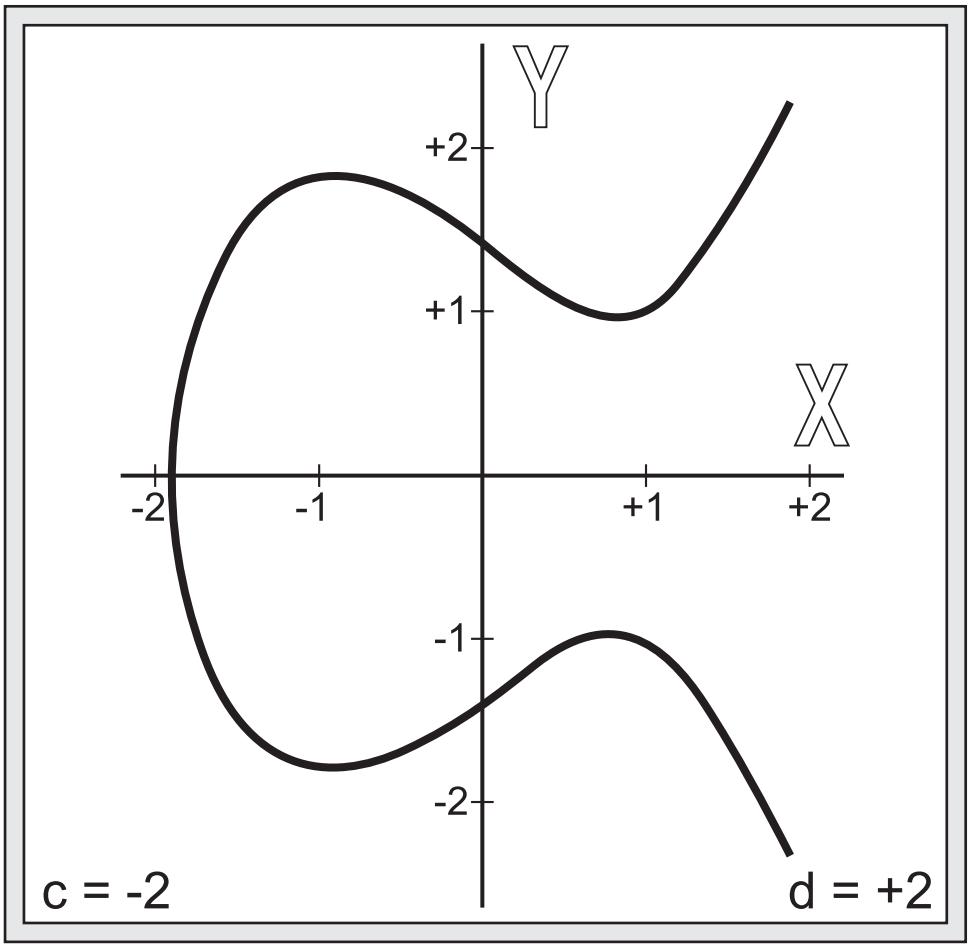
ECDH

1.0 Criptografia de Curva Elíptica

Curvas elípticas são definidas por $y^2 = x^3 + cx + d$, $4c^3 + 24d^2 \neq 0$, sendo os pontos gerados formadores de um grupo abeliano. Isso permite que as chaves criptográficas, tidas como pontos da curva elíptica, possam ter um menor número de caracteres (bits) para um nível de segurança.

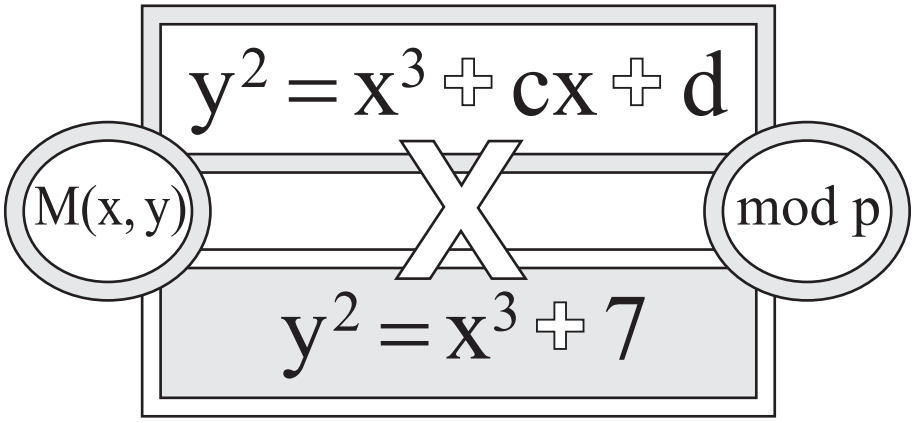
Seja a curva elíptica desenhada para $c = -2$ e $d = +2$:

$$y^2 = x^3 - 2x + 2$$



Whitfield Diffie - 1976 - Martin Hellman

3.1 Protocolo de Senhas do Bitcoin



Curva Elíptica SECP 256k1

c = 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

d = 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000007

p = $2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$

p = 115792089237316195423570985008687907853 269984665640564039457584007908834671663

M = (55066263022277343669578718895168534326250603453777594175500187360389116729240, 32670510020758816978083085130507043184471273380659243275938904335757337482424)

1. Ale Sorteia "a" (Secret Key)

a = (22863830794239430457181719345925261636721459980975062899854186166352717994614)

Ale publica A = a · M = (100511909013792440921004616255375467288314272932504506694144492508795158251272L, 80793930437443583145209246086235225250163288201968009128979181971462227091627L)

2. Bia Sorteia "b" (Secret Key)

b = (55878090536019805699189393316764628261950669774268806880198302505559525524662)

Bia publica B = b · M = (95319553509663106425946906065706938642858516945559549074668924064350234043991, 14878787532781575315860278007878723899441447428375229553873749365959100637785)

3. Troca de Chaves A⇒B e A⇐B

KA = (43724227137660311770947265141465839863589526330438943250362380944575066182837, 17929074617303098697117295968885557522267165921417751639750319187916693416130)

Ale executa a operação modular KA = a · (bM)

KB = (43724227137660311770947265141465839863589526330438943250362380944575066182837, 17929074617303098697117295968885557522267165921417751639750319187916693416130)

Bia executa a operação modular KB = b · (aM)

4. A chave pública compartilhada entre Ale e Bia é a componente x de K (x, y)

X = (43724227137660311770947265141465839863589526330438943250362380944575066182837)

Troca de Chaves Elípticas