1. Non-malleability is the property by which an adversary cannot transform the ciphertext C^* to be decrypted into another ciphertext $C' (\neq C^*)$ such that

$$Dec(C') = f(Dec(C^*))$$

(the decryptions are related to each other).

In ECC : $PR = k$ $PB = K = kG$.

Enc(m) : ~~$C_1 = k$~~ choose r

$C_1 = rG$ $C_2 = m + rK$.

Dec(m) :

$m = C_2 + (-kC_1)$ (k is private).

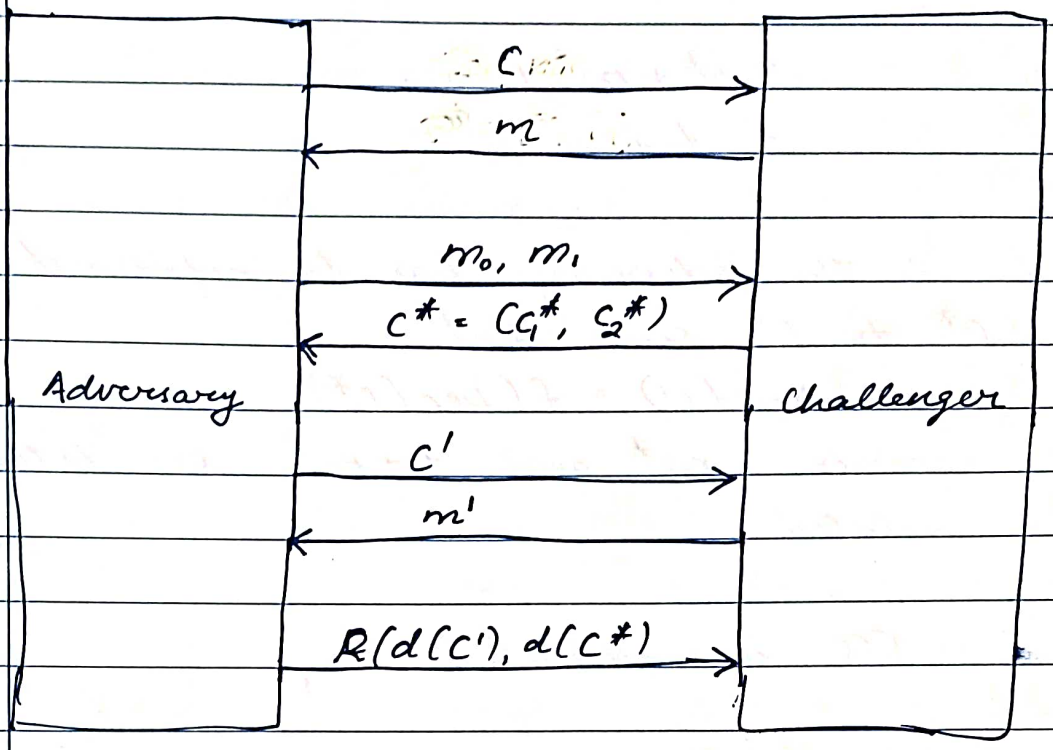
$= m + rK + (-k.rG)$

$= m + rK + (-rkG)$

$= m + rK + (-rK)$

$= m + \infty$ $(P + (-P) = \infty)$

$= m$ $(P + \infty = P)$.



Adversary has $c^* = (C_1^*, C_2^*)$

$= (r^* G, m^* + r^* K)$.

He can find $c' = (C_1^*, t + C_2^*)$ where t is a random point on the ECC

$C_1' = C_1^*$

$= r^* G$

$C_2' = t + C_2^*$

$= t + m^* + r^* K$

$C_2' + (-k C_1')$

$= \cancel{t + C_2^* +}$

$= t + m^* + r^* K + (-k r^* G)$

$= t + m^* + r^* K + (-r^* k G)$

$= t + m^* + r^* K + (-r^* K)$

$= t + m^* + \infty$

$= t + m^*$

$\therefore$ The adversary has transformed C^* to C' such that

$Dec(C') = f(Dec(C^*))$

since m^* and $t + m^*$ are both related

$\therefore$ ECC is malleable

2. $x^3 + x + 1$

Additive inverse :

$f + f^{-1} =$ Additive identity

$= 0$

$\therefore x^3 + x + 1 + (x^3 + x + 1)^{-1} = 0$

$(x^3 + x + 1)^{-1} = -x^3 - x - 1$

$\equiv x^3 + x + 1 \pmod 2$

$x^3 + x + 1 + (x^3 + x + 1)^{-1} = x^3 + x + 1 + x^3 + x + 1$

$= (1+1)x^3 + (1+1)x + (1+1)$

$\equiv 0x^3 + 0x + 0$

$= 0$

$\therefore$ Additive inverse of $x^3+x+1 = x^3+x+1$.

Multiplicative inverse :

	q	x_x	x_y
x^5+x+1		1	0
x^3+x+1	x^2+1	0	1
x^2	x	1	$-x^0-1 \equiv x^2+1$
$x+1$	$x+1$	$-x \equiv x$	$1-x(x^2+1)$ $\equiv x^3+x+1$
1	$x+1$	$1-x(x+1)$ $\equiv x^2+x+1$	$(x^2+1)-(x+1)(x^3+x+1)$
0			

$$x^3+x+1 \overline{)\, x^5+x+1 \,(\, x^2+1}$$
$$\underline{(-)\ x^5+x^3+x^2}$$
$$-x^3-x^2+x+1$$
$$\equiv x^3+x^2+x+1 \pmod 2$$
$$\underline{(-)\ x^3+x+1}$$
$$x^2$$

$$x^2 \overline{)\, x^3+x+1 \,(\, x}$$
$$\underline{(-)\ x^3}$$
$$x+1.$$

$$x+1 \overline{)\, x^2}$$

$$\underline{(-)\ x^2 + x}$$

$$-x$$

$$\equiv x \pmod 2$$

$$\underline{(-)\ \ x+1}$$

$$-1$$

$$\equiv 1 \pmod 2$$

$$b = (x^2+1) - (x+1)(x^3+x+1)$$

$$= x^2+1 - (x^4+x^3+x^2+(1+1)x+1)$$

$$= x^2+1+x^4+x^3+x^2+1$$

$$= x^4+x^3+(1+1)x^2+(1+1)$$

$$= x^4+x^3$$

$\therefore (x^3+x+1)^{-1} \bmod x^5+x+1 = x^4+x^3$

(multiplicative inverse)

Check :

$$(x^3+x+1)(x^4+x^3+1) = x^7+x^6+x^5+x^4+x^4+x^3+x^3+x+1$$

$$= x^7+x^6+x^5+x+1$$

$$x^7 + x^4+x^2$$

$$x^5+x^2+$$

$$x^6+x^5+x^4+x^2+x+1$$

$$x^6 \quad +x^3+x$$

$$x^5+x^4+x^3+x^2+1$$

3. $y^2 = x^3 + x + 6$. $\quad p = 11$

i) $P(x_3, y_3) + Q(x_4, y_4)$.

Given $x_3 \neq x_4$.

$\Rightarrow P \neq Q$.

If $Q = \infty$

$$P + Q = P + \infty = P(x_3, y_3).$$

If $P = \infty$

$$P + Q = \infty + Q = Q(x_4, y_4)$$

Else :

Draw a line passing through P and Q it intersects the curve against at $R'(x_5, -y_5)$

The answer to $P + Q = -R' = R(x_5, -(-y_5))$

$$= R(x_5, y_5).$$

slope of line passing through P and Q is

$$m = \frac{y_4 - y_3}{x_4 - x_3} \longrightarrow (1)$$

which can be found since $P(x_3, y_3)$ and $Q(x_4, y_4)$ are known

we know that equation of line through P, Q is $y = mx + c$

$$y^2 = x^3 + x + 6$$

$$\Rightarrow (mx + c)^2 = x^3 + x + 6$$

$$x^3 - m^2x^2 \mp 2cmx \mp c^2 + x + 6 = 0$$

$$x^3 - m^2x^2 + (1 - 2cm)x + (6 - c^2) = 0$$

sum of roots

$$x_1 + x_2 + x_3 = \frac{-(-m^2)}{1} = m^2$$

we know that $x_1 = x_3$ and $x_2 = x_4$ are roots since the line passes through P and Q

Ally $x_3 = x_5$ (for point R' on the line)

$\therefore$ ~~$x_4 +$~~

$$x_3 + x_4 + x_5 = m^2$$

$$\Rightarrow x_5 = (m^2 - x_3 - x_4) \bmod 11$$

Now $R'(x_5, -y_5)$

$$\Rightarrow m = \frac{-y_5 - y_1}{x_5 - x_1}$$

~~y_1~~

$$-y_5 - y_1 = m(x_5 - x_1)$$

$$y_5 = (m(x_1 - x_5) - y_1) \bmod 11$$

$\therefore P + Q = R(x_5, y_5)$

where $x_5 = (m^2 - x_3 - x_4) \bmod 11$

$y_5 = (m(x_1 - x_5) - y_1) \bmod 11$

and $m = \dfrac{y_4 - y_3}{x_4 - x_3}$.

$= (y_4 - y_3)(x_4 - x_3)^{-1} \bmod 11$.

(ii) Let P, Q, R be 3 points on the straight line
Let R be $R(x_3, y_3)$.

By above definition

$P + Q = R'(x_3, -y_3)$. (conjugate of R).

$= -R$

2 3

Add R on both sides

$P + Q + R = (R) + R$

$P + Q + R = \infty$

4. Modified El Gamal

choose k

$C_1 = g^k$ $\qquad$ $C_2 = my^k$

$m = C_2$

4. Modified El Gamal

PR : x $\qquad$ PB : $g^x \bmod p = y$

choose $k \in \{2, \ldots, p-2\}$

$C_1 = g^k$ $\qquad$ $C_2 = my^k$

$= m(PB)^k$

$m = \dfrac{C_2}{C_1^x}$

DDH :

Given g^x, g^y, g^z, it is hard to check whether $z = xy$ or not.

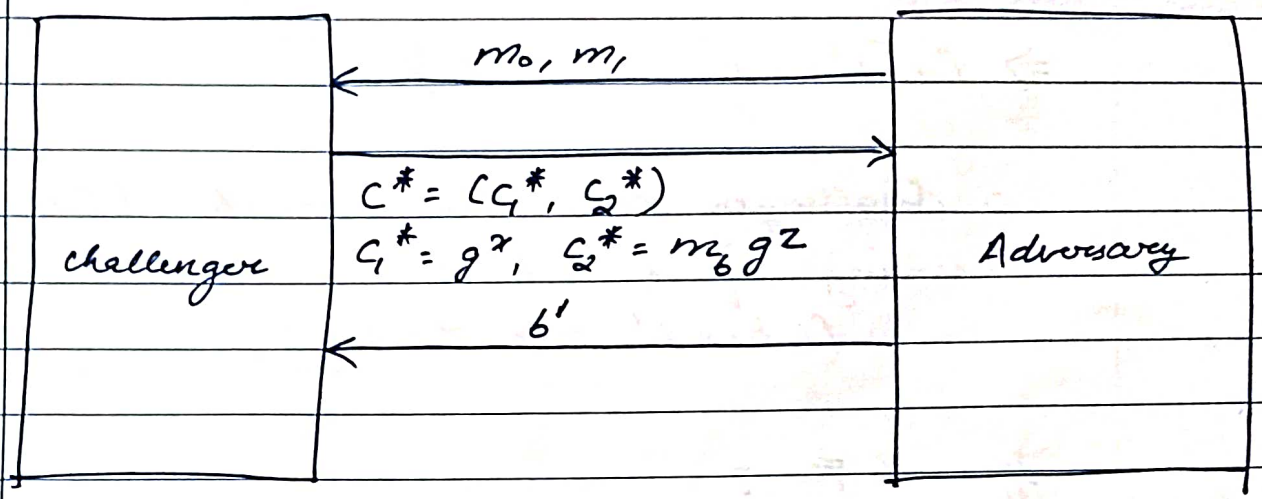
To prove : DDH is hard $\Rightarrow$ modified El-Gamal is IND-CPA secure

(A) (B)

We prove the contrapositive $\neg B \Rightarrow \neg A$

ie if an adversary can break modified El Gamal in IND-CPA, then there exist another adversary that can solve the DDH problem in feasible time with non-negligible probability

~~We consi~~ Given g^x, g^y, g^z



Assume Public key is ~~g^{xy}~~ g^z and $k = x$

$c_1 = g^k$ and $c_2 = m(y^k)$ becomes

$$c_1^* = g^x \quad , \quad c_2^* = m(g^y)^x$$
$$= m(g^{xy}).$$

If $z = xy$, then $g^z = g^{xy}$

So the challenger sends

$$c_1^* = g^x \qquad c_2^* = m_b g^z$$

Since adversary can break El-Gamal in IND-CPA,

if $z = xy$, the ciphertext is the correct encryption of m_b which the adversary can

find

$\Rightarrow Pr[b' == b] = 1 \quad > 1/2$

$\therefore$ Challenger can thus break DDH by checking if $b == b'$

$(b == b' \Rightarrow z = xy)$.

If $z \neq xy$

the encryption is not correct encryption of m_b

$\Rightarrow$ adversary predicts b' randomly ~~but with non-negligible~~

$\Rightarrow Pr[b == b'] = 1/2$.

$\Rightarrow$ ~~$Pr[z =$~~

$\Rightarrow Pr[$determining whether $z = xy$ or not$] = 1/2$

$>$ negligible

So even in this case, the challenger can predict if $z = xy$ or not with non-negligible probability

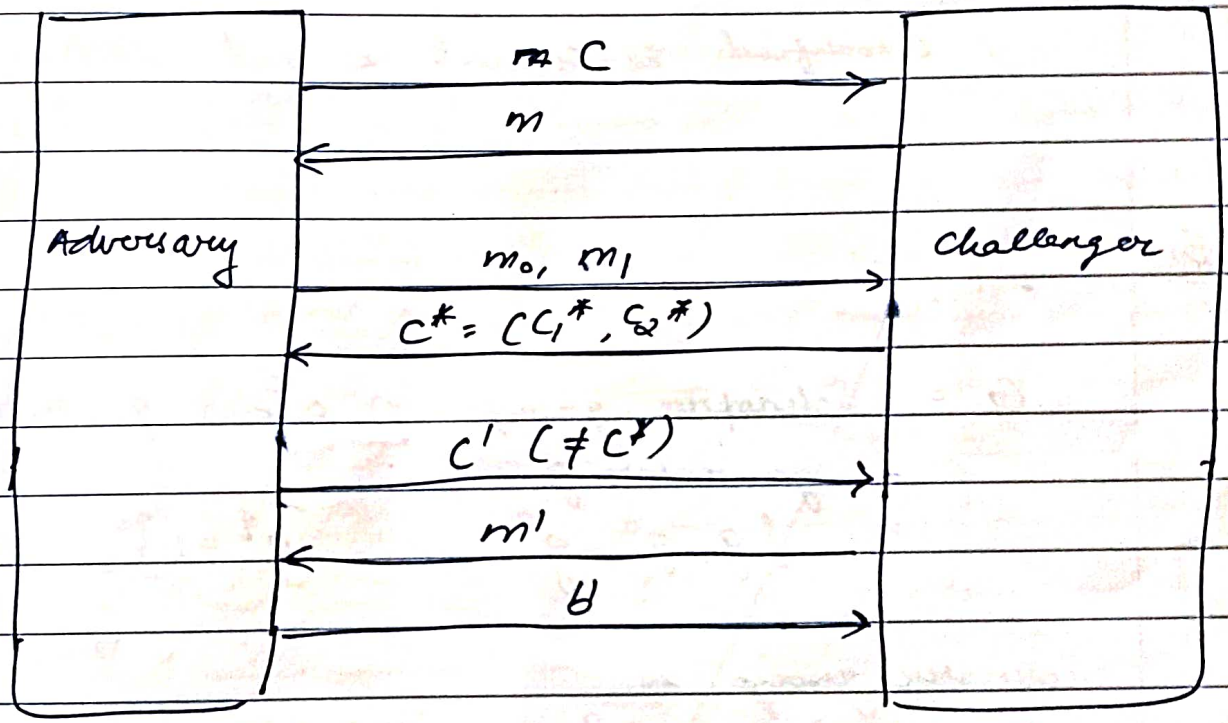
$\Rightarrow$ He can break DDH

Thus if modified El-Gamal is not IND-CPA secure, we can break DDH.

But we know that DDH assumption holds
⇒ modified El-Gamal is IND-CPA secure

$$C_1 = g^k \qquad C_2 = my^k$$

Choose random number r



Adversary can construct
$C' = (C_1', C_2')$ where

$$C_1' = C_1 = g^k \qquad C_2' = rC_2 = rmy^k.$$

$$\text{Dec}(C'): \frac{C_2'}{(C_1')^x} = \frac{rmy^k}{g^{kx}} = \frac{rmg^{kx}}{g^{kx}} = rm$$

Thus adversary gets back
$m' = r \cdot m$
and he also knows m

$\Rightarrow m = r^{-1} m'$ can be found

$\Rightarrow Pr[b' == b) = 1$ "

$\therefore$ modified El-Gamal is not IND-CCA secure

5. $q \mid p-1$.

G = Schnorr group of order q with generator g

$= \{g, g^2, g^3, \ldots, g^q = 1\}$.

Schnorr group is

$\{g, g^2, g^3, \ldots, g^q = 1\}$.

Given (g, g^x), find (c, c^x) of any element c in G.

we know that every element $c \in G$ can be written as $c = g^i$ $\quad i \in \{1, 2, \ldots, q\}$.

$\therefore (c, c^x) = (g^i, (g^i)^x)$

$= (g^i, (g^x)^i)$

$\therefore$ ~~$c = g^i$ and~~

$\therefore$ we just find $(g, g^x)^i = (g^i, (g^x)^i)$

$= (c, c^x)$.

(Written at the end)

6. $x \equiv y \bmod p$

$x \equiv y \bmod q$

Let $N = pq$

$n_1 = p \qquad n_2 = q$

$N_1 = \frac{N}{n_1} \qquad N_2 = \frac{N}{n_2}$

$= q \qquad = p.$

By CRT

$x = [y \cdot N_1 (N_1^{-1} \bmod n_1) + y \cdot N_2 (N_2^{-1} \bmod n_2)] \bmod N$

$= [y[q(q^{-1} \bmod p) + p \cdot (p^{-1} \bmod q)] \bmod N$

we know that GCD$(p, q) = 1$

$\Rightarrow q(q^{-1} \bmod p) + p(p^{-1} \bmod q) = 1$ (By Extended Euclidean algorithm).

$\therefore x = y \cdot 1 \bmod N$

$= y \bmod N$

5. $p = 11$

$q = 5$

$q \mid p-1.$

$G = \{g^1, g^2, g^3, g^4, g^5\} \bmod 11.$

~~$11 = 2 \times 5 + 1$~~

~~$p =$~~

$11 = 5 \times 2 + 1$

$p = q \times r + 1$

$r = 2$

Choose $h \in \{1, \ldots, p\}$

Let $h = 2$

$h^r = 2^2 = 4 \neq 1 \bmod 11.$

$\therefore h = 2$

$g = h^r = 2^2 = 4.$

$G = \{4^1, 4^2, 4^3, 4^4, 4^5\}.$

$4^1 \downarrow 4$, $4^2 \downarrow 5$, $4^3 \downarrow 9$, $4^4 \downarrow 3$, $4^5 \downarrow 1$

$G = \{4, 5, 9, 3, 1\}$ is the Schnorr group.

Given $(g, g^x) = (4, 4^x)$

Any element $c \in G$ can be written as

$c = 4^i$ where $i = \{1, 2, \ldots, q\}$.

$= \{1, 2, 3, 4, 5\}$.

$$(c, c^x) = (4^i, (4^i)^x)$$
$$= (4^i, (4^x)^i)$$
$$= (g^i, (g^x)^i)$$
$$= (g, g^x)^i \bmod p$$

~~$i = c$~~

~~$c = g^i$~~ ~~$c^x = (g^x)^i$~~

$$\{(c, c^x) \mid c \in G\} = \{(g, g^x)^i \mid i = \{1, 2, 3, 4, 5\}\}$$

$c = g^i \bmod p$

But given ~~$c = g^i$~~, it is hard to find i (~~Compact~~ Discrete logarithm problem).