1) RSA Practice

a) $p=5$, $q=11$, $e=9$

$N = pq \rightarrow 55$

d- inverse $e(\text{mod}(p-1)(q-1))$

$= 9^{-1}(\text{mod}(4)(10))$

$= 9^{-1}(\text{mod } 40)$

$9x \equiv 1 (\text{mod } 40)$

$x = 9$

$\boxed{d = 9}$

b) $E(x) \equiv x^e (\text{mod } N)$

$y = E(x)$

$x = D(y) \equiv y^d (\text{mod } N)$

$y^d (\text{mod } N)$

$\equiv 4^9 (\text{mod } 55)$

$\equiv 262144 (\text{mod } 55)$

$\boxed{x \equiv 14 (\text{mod } 55)}$

c) $E(x) \equiv 14^9 (\text{mod } 55)$

$\equiv (14 \cdot 14^8)(\text{mod } 55)$

$\equiv (14)(14^2)^4 (\text{mod } 55)$

$\equiv (14)(196)^4 (\text{mod } 55)$

$\equiv 14 \cdot 31^4 (\text{mod } 55)$

$\equiv 14 \cdot 16 (\text{mod } 55)$

$\equiv 224 (\text{mod } 55)$

$\boxed{y \equiv 4 (\text{mod } 55)}$

2) Tweaking RSA

a) $N = p$ Show $D(E(x)) = x$

$e \rightarrow$ usually a number relatively prime to $(p-1)(q-1)$
instead:

$p = 5$: $(p-1) \rightarrow (5-1) = 4$

$\gcd(e, 4) = 1$

$\boxed{e = 3}$

Assume message $x = 13$

$E(x) \equiv 13^3 \pmod 5$
$\equiv 2197 \pmod 5 \equiv 2 \pmod 5$

$d: 3^{-1} \pmod 4$
$3x \equiv 1 \pmod 4$
$\equiv 3 \pmod 4$

$y = 2$; $d = 3$

$D(y) \equiv 2^3 \pmod 5$
$\equiv 8 \pmod 5 \equiv 3($mo

b) We know that p & q are not known to the world, only (N, e) which is the public key is accessible to the public (and also Eve). To compute d, we would usually need to find $e^{-1} (\bmod (p-1)(q-1))$. However, since $N = p$, and Eve knows N, she also knows p and can now just compute $e^{-1} (\bmod (p-1))$ using Euclid's extended algorithm.

c) $N = pqr$

Encryption: $E(x)$

modification to e:

- instead compute a number relatively prime to $(p-1)(q-1)(r-1)$

x- message

$E(x) \equiv x^e \pmod N$

Decryption:

modification to d:

instead compute inverse of $e \pmod{(p-1)(q-1)(r-1)}$

$y = E(x)$

$x = D(y) \equiv y^d \pmod N$

Prove:

↳ $(x^e)^d \equiv x \pmod N$ where $N = (p-1)(q-1)(r-1)$, for every $x \in \{0, 1, \dots N-1\}$

$ed \equiv 1 \pmod{(p-1)(q-1)(r-1)}$

$ed = 1 + k(p-1)(q-1)(r-1)$

Claim: $p \mid x(x^{k(p-1)(q-1)(r-1)} - 1)$;

consider:

case 1 - x not multiple of p:

Since $x \not\equiv 0 \pmod p$, use FLT to find $x^{p-1} \equiv 1 \pmod p$.

thus, $x^{k(p-1)(q-1)(r-1)} - 1 \equiv 0 \pmod p$

case 2 - x is a multiple of p, then x clearly is divisible by p.

$x(x^{k(p-1)(q-1)(r-1)} - 1)$ is also divisible by q, and therefore also divisible by p, q, and r. Since $p, q,$ and r are primes, they also must be divisible by their product, $pqr = N$, which implies the expression is equal to $0 \pmod N$, which would give us back correctly the original message.

3) Secret Sharing

Construct 3 polynomials

i) TA + TA :

$p(x)$, where $p(x)$ has degree $d=1$

$p(0)=S$

TA 1 : $p(1)$
TA 2: $p(2)$

ii) R + R + R :

$q(x)$, $d=2$
$q(0) = S$

R1 : $q(1)$
R2: $q(2)$
R3: $q(3)$

iii) TA + R :

$r(x)$, $d=2$
$r(0) = S$

TA 1: $r(1)$
TA 2: $r(1)$
R1 : $r(2)$
R2: $r(2)$
R3: $r(3)$

each share corresponds to a different polynomial

4) One Point Interpolation

a) $p(x) = x^k + a_{k-1}x^{k-1} + \dots a_1x^1 + a_0$

if we're given: (x_0, y_0)
(x_1, y_1)
(x_2, y_2)
$\vdots$
(x_k, y_k)

$p(x)$ at $x = x_1$: $y_1 = x_1^k + a_{k-1}x_1^{k-1} + \dots a_1x^1 + a_0$

$$\underbrace{y_1 - x_1^k}_{\text{known}} = \underbrace{a_{k-1}x_1^{k-1} + \dots a_1x_1^1 + a_0}_{\text{unknown}}$$

for $p(x)$ for inputs x_0 to x_k, we can rearrange $p(x)$ w/ degree k to a polynomial $g(x)$ w/ degree $k-1$.

now, for $g(x)$ with $k-1$ degree, we are able to use k points to use LaGrange Interpolation, since $k+1$ points uniquely determine a degree k polynomial, and $k-1+1 = k$.

Using LaGrange interpolation for set of inputs $(x_i, g(x_i))$, we can now determine $f(x)$.

b) Assume coefficient c_i, where $0 \le c_i < 100$ $\forall i \in [0, k-1]$

for $x_* > c_i$:

$f(x_*) = x^i + c_{i-1}x^{i-1} + \dots c_1x^1 + c_0$

consider:

$f(x_*) = 12x_*^2 + 11x_* + 32$

for $x_* = 100$:

$\downarrow$

$= 12(100^2) + 11(100) + 32$

$= 12(10{,}000) + 11(100) + 32$

$= 120{,}000 + 1{,}100 + 32$

$\boxed{f(x_*) = 121{,}132}$

note: this would not work for $c_i > x_*$

5) Lagrange? More like Lamegrange.

a) Interpolate through (x_0, y_0)

$$P(x) = y_0$$

(the other leading coefficients have 0)

degree $d = 0$

b) $f_0(x) = y_0$

$f_1(x) = f_0(x) + a_1(x - x_0)$ } passes through (x_0, y_0) and (x_1, y_1)

$d = 1$

evaluate: $f_1(x)$ at $x = x_0$

$$f_1(x) = f_0(x_0) + a_1(x_0 - x_0)$$

since $f_0(x_0) = y_0$

$$= y_0 + a_1(0)$$

$$= y_0$$

$f_1(x)$ at $x = x_1$

$$f_1(x) = f_0(x_1) + a_1(x_1 - x_0)$$

$$= f_0(x_1) + a_1(x_1 - x_0)$$

$$y_1 = y_0 + a_1(x_1 - x_0)$$

$$(y_1 - y_0) = a_1(x_1 - x_0)$$

$$\boxed{a_1 = \frac{(y_1 - y_0)}{(x_1 - x_0)}}$$

c) $f_2(x) = f_1(x) + a_2(x - x_0)(x - x_1)$ for $(x_0, y_0), (x_1, y_1)$ and (x_2, y_2)

eval: $f_2(x)$ at $x = x_2$

$$f_2(x_2) = f_1(x_2) + a_2(x_2 - x_0)(x_2 - x_1)$$

$$y_2 = f_1(x_2) + a_2(x_2 - x_0)(x_2 - x_1)$$

$$y_2 - f_1(x_2) = a_2(x_2 - x_0)(x_2 - x_1)$$

$$\boxed{a_2 = \frac{(y_2 - f_1(x_2))}{(x_2 - x_0)(x_2 - x_1)}}$$

d) $f_{i+x}(x) = f_i(x) + a_{i+1} \prod_{j=0}^{i} (x - x_j)$

we know $f_i(x)$ passes through points $(x_0, y_0), \ldots (x_i, y_i)$. we can set $f_{x_{i+1}}(x)$ equal to the original equation for the polynomial, evaluated at x_{i+1}.

we know that $f_{i+1}(x)$ passes through (x_{i+1}, y_{i+1}), so we can set $f_{x_{i+1}}(x) = y_{i+1}$.
The polynomial will be of some form:

$$y_{i+1} = f_i(x_i) + a_{i+1}(x - x_0)(x - x_1) \ldots (x - x_{i-1})$$

Since we know $f_i(x_i)$, we can substitute the value for $f_i(x_i)$ into the equation for the polynomial and solve for a_{i+1}.

Therefore, a_{i+1} will take on some value:

$$f_{i+1}(x) = f_i(x) + a_{i+1} \prod_{j=0}^{i} (x - x_j)$$

$$\boxed{a_{i+1} = \frac{y_{i+1} - f_i(x_{i+1})}{\prod_{j=0}^{i} (x_{i+1} - x_j)}}$$

6) Equivalent Polynomials

$GF(p) \rightarrow \{0, \dots p-1\}$ $\quad a^{p-1} \equiv 1 (\mod p)$

$f(x) \equiv g(x) (\mod p)$

$GF(5) = \mod 5$

$f(x) \equiv x^5 (\mod 5)$

$x^5 \equiv f(x)(\mod 5)$

$x \cdot x^4 \equiv f(x)(\mod 5)$

$\boxed{x \equiv f(x)(\mod 5)}$

Check: $\{0, 1, 2, 3, 4\}$

$0^5 = 0 = 0(\mod 5)$

$1^5 = 1 = 1(\mod 5)$

$2^5 = 32(\mod 5) = 2(\mod 5)$

$3^5 = 243(\mod 5) \equiv 3(\mod 5)$

$4^5 = 1024(\mod 5) \equiv 4(\mod 5)$

$g(x) = 4x^{70} + 9x^{11} + 70 \ (\mod 11)$

$70 \rightarrow 4(\mod 11)$

$4(x^{10})^7 \qquad 9x \cdot x^{10}$

$4(1)^7 = 4 \qquad = 9x$

$\underbrace{\qquad\qquad\qquad}_{4 + 9x + 4}$

$\boxed{= 9x + 8}$

$9(1) + 8 = 17(\mod 11)$ ✓

$= 6(\mod 11)$

$4 + 9 + 70 (\mod 11)$ ✓

$83(\mod 11)$

$6(\mod 11)$

b) Given $GF(p)$, we know we are working w/ finite field $(\mod p)$, where $f(x) \equiv g(x)(\mod p)$, where $\bar{f}(x) \equiv g(x)$.

Say we are given a polynomial w/ degree p, it follows that $f(x)$ is in the form

$$a_p x^p + \dots a_1 x^1 + a_0 \ (\mod p)$$

we can reduce each term w/ degree $\geq p (\mod p)$ to a smaller term.

Consider: $a_p x^p \equiv a_p x \cdot x^{p-1}$

we know from FLT that $x^{p-1} \equiv 1 (\mod p)$, so we are always able to reduce a smaller $p-1$ degree term from a degree $\geq p$ term. doing this for every degree $\geq p$ term, we get a polynomial w/ leading coefficient $< p$, meaning degree $\bar{f}(x) = g(x) < p$.