Exam 2 Comments

10/31/16 (1)
10/28/16

$$\begin{array}{rl} 02\times C9 & = x\cdot(f(x)) \\ +\ 02\times C9 & x\cdot(f(x)) \\ \hline & 2x\cdot(f(x) \quad \text{each coeff mod 2} \\ & \equiv 0x\cdot f(x)) \\ & \equiv \boxed{0} \end{array}$$

$$\begin{array}{rl} 03\times C9 & = (x+1)\,f(x) \\ +\ 01\times C9 & = \quad 1\ f(x) \\ \hline & (x+2)\,f(x) \\ & \equiv (x+0)\,f(x) \\ & \equiv x f(x) \quad = 02\times C9. \end{array}$$

$$\begin{aligned} 04\times C9 &= x^2\cdot f(x) \\ &= x(x\cdot f(x)) \\ &= 02\times(02\times C9) \\ &= 02\times(89) \\ &= \boxed{09} \end{aligned}$$

$\phi(mn) = \phi(m)\phi(n)$ ONLY WORKS IF $\gcd(m,n)=1$.

$\phi(10\times 9) \neq \phi(3)\times\phi(30)$
$= \phi(10)\times\phi(9)$

$\phi(10!) = 2\times 3\times 2^2\times 5\times 2\times 3\times 7\times 2^3\times 3^2\times 2\times 5$
$= 2^8\times 3^4\times 5^2\times 7^1$

~~10/31/16~~ (2)
10/28/16

RSA Encryption

Alice wants to set up keys so anyone can send her a message.

1. Alice generates to large primes p and q. These are private keys.
2. Calculate $n = pq$ and $\phi(n) = (p-1)(q-1)$. n is public. $\phi(n)$ is private (not a key).
3. Pick a value e such that $\gcd(e, \phi(n)) = 1$. e will be a public key.
4. Calculate $d = e^{-1} \bmod \phi(n)$, using EEA (extended Euclidean algorithm). ($ed \equiv 1 \bmod \phi(n)$.) d is private key

For Bob send a message to Alice, he calculates $C = M^e \bmod n$

Alice decrypts by calculating $C^d = M \bmod n$

$(M^e)^d \equiv M \bmod n$ [Need to Prove]

Note: we require $\gcd(M, n) = 1$.

$$(M^e)^d = M^{ed} = M^{k\phi(n)+1} = M^{k\phi(n)} \times M^1$$
$$= (M^{\phi(n)})^k \times M^1$$
$$\equiv 1^k \times M^1 \bmod n$$
$$\equiv M \bmod n$$

~~10/31/16~~ (3)
10/28/16

$p = 7, q = 17$

$n = 119$

$\phi(n) = (7-1)(17-1) = 96$

$e = 55$

$d = 55^{-1} \bmod 96$

$96 = 1 \times 55 + 41$
$55 = 1 \times 41 + 14$
$41 = 2 \times 14 + 13$
$14 = 1 \times 13 + 1$

$14 - 1 \times 13 = 1$
$14 - (41 - 2 \times 14) = 1$
$14 - 41 + 2 \times 14 = 1$
$3 \times 14 - 1 \times 41 = 1$
$3(55 - 41) - 1 \times 41 = 1$
$3 \times 55 - 4 \times 41 = 1$
$3 \times 55 - 4(96 - 55) = 1$
$3 \times 55 - 4 \times 96 + 4 \times 55 = 1$
$7 \times 55 - 4 \times 96 = 1$

$55^{-1} \equiv 7 \bmod 96$

$\boxed{d = 7}$

Send $M = \boxed{32}$

$C = 32^{55} \bmod 119 = 25$

$M \equiv 25^{7} = \boxed{32} \bmod 119$