Homework

① GF(5) @ $(2x+3)-(2x^3+3x-2)$

$-2x^3-x+5 \quad -2x^3-x = \boxed{3x^3+4x}$

ⓑ $(3x^3+x-2)\times(x^2+4x+3)$

$3x^5+12x^4+9x^3+x^3+4x^2+3x-2x^2-8x-6$

$3x^5+12x^4+10x^3+2x^2-5x-6 = \boxed{3x^5+2x^4+2x^2+4}$

② GF(11) @ $(2x+3)-(-2x^3+3x+2)$

$-2x^3-x+5 = \boxed{9x^3+10x+5}$

ⓑ $(3x^3+x-2)\times(x^2+4x+3)$

$3x^5+x^4+10x^3+2x^2-5x-6 = \boxed{3x^5+x^4+10x^3+2x^2+6x+5}$

③ $GF(2^3)$ with $f(x)=x^3+x+1$ $\{0,1,x,x+1,x^2,x^2+1,x^2+x,x^2+x+1\}$

@ $(x^2+x+1)(x+1)=x^3+2x^2+2x+1$ ⓑ $(x^2+1)-(x^2+x+1)=\boxed{x}$

$x^3+x+1 \;\overline{)\; x^3+2x^2+2x+1}$ (1)

$-x^3+x+1$

$2x^2+x = \boxed{x}$

ⓒ $(x^2+x+1)(x^2+1)=x^4+x^3+2x^2+x+1$

$x^3+x+1 \;\overline{)\; x^4+x^3+2x^2+x+1}$ ($x+1$)

$-x^4+x^2+x$

x^3+x^2+1

$-x^3+x+1$

$\boxed{x^2+x}$

④ $GF(2^8)$ with $f(x)=x^8+x^4+x^3+x+1$

@ $(x^6+x+1)(x^3+1) \to x^9+x^6+x^4+x^3+x+1$

$x^8+x^4+x^3+x+1 \;\overline{)\; x^9+x^6+x^4+x^3+x+1}$ (x)

$x^9+x^5+x^4+x^2+x$

$\boxed{x^6+x^5+x^3+x^2+1}$

ⓑ $(x^6+1)-(x^6+x+1) = \boxed{x+1}$

ⓒ $(x^6+x+1)/(x^2+1)$

$(x^6+x+1)(x^6+x^4+x)$

$(x^2+1)(x^6+x^4+x)$

$x^8+x^4+x^3+x+1 \;\overline{)\; x^8+x^4+x^3+x}$ (1)

$x^8+x^4+x^3+x+1$

$-1 = \boxed{1}$

$x^6+x^4+x = \frac{1}{x^2+1}$

$x^{12}+x^{10}+x^7+x^7+x^5+x^2+x^6+x^4+x$

$x^8+x^4+x^3+x+1 \;\overline{)\; x^{12}+x^{10}+x^6+x^5+x^4+x^2+x}$

$x^{12}+x^8+x^7+x^5+x^4$

$x^{10}+x^8+x^7+x^6+x^2+x$

$x^{10}+x^6+x^5+x^3+x^2$

$x^8+x^7+x^5+x^3+x$

$x^8+x^4+x^3+x+1$

$\boxed{x^7+x^5+x^4+1}$

(5) (a) $p=3\ q=11\ e=7\ M=5\quad n=33\quad \phi(n)=20$

$7\cdot d=1 \bmod 20\quad d=3\quad C=5^7 \bmod 33\quad 5^3=125=26 \bmod 33$

$5^7=5^3\cdot5^3\cdot5=26\cdot26\cdot5\quad 26\cdot5=130=31 \bmod 33$

$14 \bmod 33=C$

decrypt $=14^3 \bmod 33=5$

$+806 \bmod 33=14$

(b) $p=5\quad q=11\quad n=55\quad \phi(n)=40\quad e=3\quad d=27\quad m=9$

$C=9^3 \bmod 55\quad 81=26 \bmod 55\quad 9\cdot26=234=14 \bmod 55$

$C=14 \bmod 55\quad m=14^{27} \bmod 55\quad 27=11011\ (((((m^2)\cdot m)^2)^2\cdot m)^2\cdot m$

$14^2=196=31 \bmod 55\cdot14=49^2 \bmod 55=36 \bmod 55\cdot14=49^2 \bmod 55=36 \bmod 55$

$36\cdot14 \bmod 55=\boxed{9}$

(c) $p=7\quad q=11\quad n=77\quad \phi n=60\quad e=17\quad d=53\quad m=8$

$e=17=10001=(((m^2)^2)^2)^2\cdot m\quad 8^2=64^2 \bmod 77=-13^2=169=15^2=71=-6^2=36$

$36\cdot8=57 \bmod 77=C\quad 53=110101\ ((((C^2)^2\cdot C)^2\cdot8^2)^2\cdot C$

$57^2=15 \bmod 77\times57=8 \bmod 77=64 \bmod 77^2=15\cdot57=8^2=64^2=75\cdot57=\boxed{8}$

(d) $p=11\quad q=13\quad \phi n=120\quad n=143\quad e=11\quad d=11\quad m=7$

$11=1011=((m^2)^2\cdot m)^2\cdot m\quad 7^2=49^2=113\cdot7=76 \bmod 143=56\cdot7$

$C=106 \bmod 143\quad 106^2=82^2=3\cdot106=32^2=23\cdot106=\boxed{7} \bmod 143$

(e) $p=17\quad q=31\quad n=527\quad \phi n=480\quad e=7\quad d=343\quad m=2$

$2^7=\boxed{128 \bmod 527}\quad 128^{343}\quad 343=101|01|0111$

$(((((128)^2)^2\cdot128)^2)^2\cdot128)^2)^2\cdot128$

$47^2=101\cdot128=280=404=373\cdot128=314=47^2=101\cdot128=280=404\cdot128=66$

$140\cdot128=\boxed{2} \bmod 527$

(6) $p=7 \quad q=5 \quad n=35 \quad \phi_n=24 \quad e=5 \quad d=5$

$C=10$

$m=10^5 \bmod 35 \qquad 5=101 = ((10^2)^2 \cdot 10$

$100 = 30 \bmod 35 \quad 30^2 = 900 = 25 \bmod 35 \cdot 10 = 250 = \boxed{5} \bmod 35$

(7) $n=3599 \quad p=59 \quad q=61 \quad \phi_n=3480 \quad e=31 \quad d=1161$

$\gcd(n, \text{mod})=1 \qquad \begin{array}{r} 31 \overline{)3480} \\ 3480 = 31(112)+8 \end{array}$

$31 = 8(3)+7$

$\underline{8 = 7(1)+1}$

$7 = 1(7)+0$

$1 = 8+7(-1)$

$1 = 8+(31+8(-3))(-1)$

$= 8(4)\ (31)(-1)$

$= (31)(-1)+(3480+31(-112))4$

$= 3480(4)+31(-449)$

$d = -449 \bmod 3480$

$\boxed{d=3031}$

(8) $\boxed{NO}$, this is not safe. If bob does not change his modulous someone could use his old public and private keys to calculate ϕn and then calculate his new private key using his new public key

(9) $M=2 \quad e=23 \quad n = \underset{p}{233} \cdot \underset{q}{241} = 56153 \quad \phi n = 55680$

$55680 = 23(2420)+20$

$23 = 20(1)+3$

$\underline{20 = 3(6)+2}$

$3 = 2(1)+1$

$2 = 1(2)+0$

$1 = 3+2(-1)$

$= 3+(20+3(-6))-1$

$= 3(7)+20(-1)$

$= 20(-1)+(23+20(-1))(7)$

$= 20(-8)+23(7)$

$= 23(7)+(55680+23(-2420))(-8)$

$= 55680(-8)+23(19360)+23(7)$

$23(-19367)$

$d = 19367$

$d = 1001011110100111$

$(m)^2 y^2 y^2 \cdot m y^2 y^2 \cdot m y^2 \cdot m y^2 \cdot m y^2 y^2 \cdot m y^2 y^2 y^2 \cdot m y^2 \cdot m y^2 \cdot m$

$(2)^2 = 4^2 = 16^2 = 256 \cdot 2 = 512^2 = 39424^2 = 256 \cdot 2 = 512^2 = 39424 \cdot 2 = 23168^2 = 1024 \cdot 2 = 2048^2 =$

$18304^2 = (9856 \cdot 2)^2 = 27904^2 = 4096^2 = (17536 \cdot 2)^2 = 18304 = 39424 \cdot 2 = \boxed{23168}$