

Imperial College London
Department of Computing

Network Security (430)

Un-assessed Coursework 1

Answer the following questions, consulting Chapter 7 of *W. Stallings, Cryptography and Network Security*. Avoid using a calculator unless suggested to do so.

0. (i) $-26 \pmod{7}$
(ii) $-371 \pmod{8}$
1. (i) $22 + 16 \pmod{5}$
(ii) $39 * 83 \pmod{5}$
(iii) $5^4 \pmod{7}$
(iv) $3^5 \pmod{7}$
2. $\gcd(540, 168)$ (You may use a calculator for this question)
3. By trying each possible multiplication with a “candidate inverse” work out the following (i.e. don’t use Euclid’s extended algorithm):
 - (i) $3^{-1} \pmod{7}$
 - (ii) $7^{-1} \pmod{9}$
 - (iii) $5^{-1} \pmod{11}$
 - (iii) $2^{-1} \pmod{4}$
4. Using Euclid’s extended algorithm work out: (Do this question last if you find it time consuming.)
 - (i) $7^{-1} \pmod{9}$
 - (ii) $7^{-1} \pmod{19}$
5. Divide $x^5 - x^4 + x^3$ by $x^3 + x^2 - x + 2$ producing the quotient and remainder.
6. Divide $x^6 + x^5 + x^2 + x$ by $x^3 + x^2 + 1$ over the field $\text{GF}(2)$ producing the quotient and remainder.
7. Given $f(x) = x^7 + x^6 + 1$, $g(x) = x^2 + x$, $m(x) = x^8 + x^4 + x^3 + x + 1$
What is $f(x) * g(x) \pmod{m(x)}$ over the field $\text{GF}(2)$

4. (i) $7^{-1} \pmod{9}$ Here's a concise tabular way of performing the computation:

Let's do columns A and B first:

A	B	C	Comments
9 (from Q)		0 (always)	
7 (from Q)	1	1 (always)	Given PrevColA=9, ColA=7 work out $9 = 7*1+2$ Set ColB=1 and NextColA=2
2	3		Given PrevColA=7, ColA=2 work out $7 = 2*3+1$ Set ColB=3 and NextColA=1
1	2		Given PrevColA=2, ColA=1 work out $2 = 1*2+0$ Set ColB=2 and stop since ColA=1

Now let's complete column C

A	B	C	Comments
9 (from Q)		0 (always)	
7 (from Q)	1	1 (always)	
2	3	8	$ColC = PrevPrevColC - PrevColB * PrevColC$ $0 - 1 * 1 = -1 = 8 \pmod{9}$
1	2	4	$ColC = PrevPrevColC - PrevColB * PrevColC$ $1 - 3 * 8 = -23 = 4 \pmod{9}$

Answer is final value in column C = 4

- (ii) $7^{-1} \pmod{19}$

A	B	C	Comments
19 (from Q)		0 (always)	
7 (from Q)	2	1 (always)	Given PrevColA=19, ColA=7 work out $19 = 7*2+5$ Set ColB=2 and NextColA=5
5	1		Given PrevColA=7, ColA=5 work out $7 = 5*1+2$ Set ColB=1 and NextColA=2
2	2		Given PrevColA=5, ColA=2 work out $5 = 2*2+1$ Set ColB=2 and NextColA=1
1	1		Given PrevColA=2, ColA=1 work out $2 = 1*1+1$ Set ColB=1 and stop since ColA=1

Now let's do Col C

A	B	C	Comments
19 (from Q)		0 (always)	
7 (from Q)	2	1 (always)	
5	1	17	$ColC = PrevPrevColC - PrevColB * PrevColC$ $0 - 2 * 1 = -2 = 17 \pmod{19}$
2	2	3	$ColC = PrevPrevColC - PrevColB * PrevColC$ $1 - 1 * 17 = -16 = 3 \pmod{19}$
1	1	11	$ColC = PrevPrevColC - PrevColB * PrevColC$ $17 - 2 * 3 = 11 \pmod{9}$

Answer is final value in column C = 11

