CSE3230 Algebra and Cryptography

Exercises Block Sample Solutions - double check before use

1 Polynomial (10%)

(1) $x^4 + x + 1$ - is the polynomial irreducible? What about primitive?
(2) $x^4 + x^3 + 1$ - is the polynomial irreducible? What about primitive?

Consider the following, let $f(x) = x^4 + x + 1 \in F_2[x]$ and $g(x) = x^4 + x^3 + 1 \in F_2[x]$. Polynomial f (respectively, g) is is irreducible if and only if there are no $h(x),\ k(x) \in F_2[x]$ with degree $1 \le d < 4$ such that $h(x) * k(x) = f(x)$ (respectively, $h(x) * k(x) = g(x)$). Hence we need to check if any multiplication of two polynomials of degree respectively 1 and 3 or both of degree 2 gives either f or g. We do not need to consider multiplications with polynomials without constant term (i.e. without a "+1"), since both f and g have it, and thus both of their supposed factors must also have it. Therefore the polynomial factors to be used in the multiplications are:

- Degree 1: $x + 1$
- Degree 2: $x^2 + 1,\ x^2 + x + 1$
- Degree 3: $x^3 + 1,\ x^3 + x + 1,\ x^3 + x^2 + 1,\ x^3 + x^2 + x + 1$

Without loss of generality, assume that $deg(h) \le deg(k)$. We need to check 7 multiplications, namely:

- 4 combinations given by $h(x) = x + 1$ and $k(x)$ being any of the 4 polynomials of degree 3
- 2 combinations when both $h(x)$ and $k(x)$ have degree 2 and $h(x) = k(x)$ and 1 combination when $h(x) \neq k(x)$

The results of the multiplications are the following:

(1) $(x + 1)(x^3 + 1) = x^4 + x^3 + x + 1$
(2) $(x + 1)(x^3 + x + 1) = x^4 + x^2 + x + x^3 + x + 1 = x^4 + x^3 + x^2 + 1$
(3) $(x + 1)(x^3 + x^2 + 1) = x^4 + x^3 + x + x^3 + x^2 + 1 = x^4 + x^2 + x + 1$
(4) $(x + 1)(x^3 + x^2 + x + 1) = x^4 + x^3 + x^2 + x + x^3 + x^2 + x + 1 = x^4 + 1$
(5) $(x^2 + 1)^2 = (x^2 + 1)(x^2 + 1) = x^4 + x^2 + x^2 + 1 = x^4 + 1$
(6) $(x^2 + x + 1)^2 = (x^2 + x + 1)(x^2 + x + 1) = x^4 + x^3 + x^2 + x^3 + x^2 + x + x^2 + x + 1 = x^4 + x^2 + 1$
(7) $(x^2 + 1)(x^2 + x + 1) = x^4 + x^3 + x^2 + x^2 + x + 1 = x^4 + x^3 + x + 1$

Since none of the above multiplications results in either $f(x)$ or $g(x)$, both polynomials are irreducible.

To verify whether they are also primitive, we need to check if one of their roots is a generator of the multiplicative group $F^*_{2^4}$. Such group is cyclic and has order $2^4 - 1 = 15 = 3 * 5$. Hence, by Lagrange's theorem we only need to check that it does not have order 3 or 5. Clearly for both polynomials the order cannot be 3, since we are working 1 in an extension field of dimension 4, and thus the first five elements of $F^*_{2^4}$ in multiplicative notation are always $0, 1, \alpha, \alpha^2, \alpha^3$. For order 5, remark that if α is a root of $f(x)$, we have that

$\alpha^4 + \alpha + 1 = 0 \rightarrow \alpha^4 = \alpha + 1$

Respectively, if α is a root of $g(x)$ we have

$\alpha^4 + \alpha^3 + 1 = 0 \rightarrow \alpha^4 = \alpha^3 + 1$

Consider now the element $\alpha^5 = \alpha * \alpha^4$. Under $f(x)$, we can rewrite this equation as

$\alpha * \alpha^4 = \alpha * (\alpha + 1) = \alpha^2 + 1$

On the other hand under $g(x)$ we can rewrite it as

$\alpha * \alpha^4 = \alpha * (\alpha^3 + 1) = \alpha^4 + 1 = \alpha^3 + \alpha + 1$

In both cases, we have that $\alpha^5 \neq \alpha$, so the order of α must be 15. Therefore, both $f(x)$ and $g(x)$ are primitive.

2 Difie-Hellman System (10%)

Alice and Bob choose (publicly) a prime number p, and a generator g of the cyclic group Z^*_p.

(1) How to select the value p? Or how to make a prime test, please give an example?

Consider using a safe prime p (p=2*q+1). Using q=5 for example we get p=2*5+1=11.

(2) Why it is important to set a prime p there?

To defend against attacks it is needed to set a prime number for the Difie Hellman algorithm to work. Safest is a large prime number.

(3) How do you check what is the order of an element (generator), based on your example?

By Lagrange's theorem, the orders of all subgroups of Z^*_p are the divisors of p - 1.

For the example;

Z^*_{11} => p-1 = 11-1 = 10. The divisors are 1,2,5 and 10.

(4) Consider Z^*_{31} and Z^*_{33} and for every possible generator, find what is its order.

Z^*_{31} => p-1 = 31-1 = 30. The divisors are 1,2,3,5,6,10,15 and 30.

Z^*_{32} => p-1 = 33-1 = 32. The divisors are 1,2,4,8,16 and 32.

(5) Please give an example of Alice and Bob Die-Hellman key exchange, based on Z^*_{31}, and a generator $g = 3$?

Assume that Alice chooses xA = 5 as a secret value, and Bob chooses xB = 9. Then, Alice sends the value y = 3^5 mod 31 = 26 to Bob, while Bob sends z = 3^9 mod 31 = 29 to Alice. Alice on her side computes k = z^xA mod 31 = 29^5 mod 31 = 30, while Bob computes k = y^xB mod 31 = 26^9 mod 31 = 30. Thus, the shared secret key is k = 30.

3 Rabin Cryptosystem (10%)

One of these solutions is the original plaintext m.
(1) Why one of the solutions should be the original plaintext, and how many possible solutions we will have?

Because by invoking the CRT, the four square roots +r, -r, +s and -s are being calculated. 4 possible solutions will be presented, of which 1 will be the original plaintext.

(2) Why are the formulas for m_p and m_q correct?

The formulas are actually $m_p = sqrt(c) mod\ p$ and $m_q = sqrt(c) mod\ q$. First, $p = 3\ mod\ 4$ implies that (p+1)/4 is an integer. The assumption is trivial for c=0 mod p. Thus we may assume that p does not divide c. Then $m^2_p = c^{(p+1)/2} = c * c^{(p-1)/2} = c * (c/p)\ mod\ p$. From c=m^2 mod p*q follows that c=m^2 mod p. Thus c is a quadratic residue modulo p. Hence (c/p)=1 and therefore m^2_p=c mod p.

(3) Consider p = 71 and q = 29. Show key generation, message m = 74 encryption, and message decryption.

(1) Key generation:
  (a) $n = p * q = 71 * 29 = 2059$
  (b) Thus the public key is *n*, while the private key is the pair (*p*,*q*)
(2) Encryption:
  (a) Let m=74 be the plaintext. The ciphertext y is obtained as follows:
  (b) $y = m^2 mod\ n \Rightarrow y = 74^2 mod\ 2059 = 5476\ mod\ 2059 = 1358$
(3) Decryption:
  (a) $m_p = sqrt(c) mod\ p \Rightarrow c^{(p+1)/4} mod\ p = 1358^{(71+1)/4} mod\ 71 = 3$
  (b) $m_q = sqrt(c) mod\ q \Rightarrow c^{(q+1)/4} mod\ q = 1358^{(29+1)/4} mod\ 29 = ERROR$
  (c) m_q can't be calculated. That is because actually, q does not honor the requirement of being congruent to 3 mod 4. Thus (29+1)/4 is not an integer.
  (d) A valid decryption will thus fail.

4 RSA (10%)

Let p = 73 and q = 37.
(1) Show with Fermat primality testing that the numbers are not composite with probability larger than 30%.

To check whether a number p (or q) is prime, we can do as follows:
1. Randomly choose a such that 1 ≤ a < p
2. If gcd(a;p) > 1, then p is composite
3. If gcd(a;p) = 1, compute u = a^p-1 mod p
If we have found k witnesses then the probability that p is composite is at most 1/(2^k)

$2^{72} \equiv 1\ mod\ 73$
$3^{72} \equiv 1\ mod\ 73$
$2^{36} \equiv 1\ mod\ 37$
$3^{36} \equiv 1\ mod\ 37$

The above 4 statements are true. Hence we can conclude that the numbers are not composite with a probability larger then 30%.

(2) Show key generation for RSA (note that e cannot be equal to 3).
(1) $N = p * q = 73 * 37 = 2701$
(2) $O(N) = (p-1) * (q-1) = 72 * 36 = 2592$

(3) Choose *e* => 1 < e < O(N) and coprime with N and O(N)
  (a) Go through primes (except 3) until it matches the above statement. Pick e = 5 - it is trivial to see that 5 is coprime with both *2701* and *2592*.
  (b) Lock (5, 2701)

(4) Choose d
  (a) $d * e\ mod\ O(N) = 1$
  (b) $5 * d\ mod\ 2592 = 1$
  (c) Calculate d = 1037
  (d) Unlock (1037, 2701)

(3) Show how to encrypt and decrypt message m = 24. For decryption, use Chinese Remainder Theorem to show how calculations can be done in a more efficient way.
(1) $c = m^e mod\ n = 24^5 mod\ 2701 = 76$
(2) $m = c^d mod\ n = 76^{1037} mod\ 2701 = 24$

(3) Using CRT
  (a) $m_1 = (c^d mod\ n) mod\ p = ((c\ mod\ p)^{d\ mod\ p-1})\ mod\ p$
  (b) $m_2 = (c^d mod\ n) mod\ q = ((c\ mod\ q)^{d\ mod\ q-1})\ mod\ q$
  (c) $m_1 = (76^{1037} mod\ 2701) mod\ 73 = ((76\ mod\ 73)^{1037\ mod\ 73-1})\ mod\ 73$
    (i) $m_1 = 3^{29} mod\ 73$
    (ii) $m_1 = 24$
  (d) $m_2 = (76^{1037} mod\ 2701) mod\ 37 = ((76\ mod\ 37)^{1037\ mod\ 37-1})\ mod\ 37$
    (i) $m_2 = 2^{29} mod\ 37$
    (ii) $m_2 = 24$
  (e) Combing both m_1 and m_2 - because both m_1 and m_2 are equal to 24 it is trivial to see that that is directly the decrypted answer.

5 ElGamal Signature (10%)

Consider the Elgamal signature scheme with p = 47 and generator g = 3 for Z^*_{47}. Moreover, assume that Alice chose the secret value a = 113.
(1) Show the key generation.
  (1) $\beta = g^a mod\ p$
  (2) $\beta = 3^{113} mod\ 47$
  (3) $\beta = 21$

(2) Suppose Alice wants to sign the message x = 109 and chooses k = 103 as a random value. Show how to sign the message and the corresponding signature.
(1) $gcd(k, p-1) = gcd(103, 46) = 1$
(2) $\gamma = g^k mod\ p = 3^{103} mod\ 47 = 4$

(3) $\delta = (x - a\gamma)k^{-1} mod\, p - 1 = (109 - 113 * 4) * 103^{-1} mod\, 46 = (-343) * 21\, mod\, 46 = 19$
(4) Thus, we have the signature pair for the message (4, 19)

(3) Please show the verification for the above signature.

The verification process is checking whether $g^m = y^\gamma r^\delta\, mod\, p$

(1) $g^m mod\, p = 3^{109} mod\, 47 = 2$
(2) $\beta^\gamma r^\delta mod\, p = 21^4 * 4^{19} mod\, 47 = 2$
(3) Since the above two parts are equal, (4, 19) is a valid digital signature for the message m = 109.

6 Fermat Primality Test (10%)

Please select a number (which could be random 3-digits number) and run the Fermat primality test for the number.
Is the number a composite? If not, how many witnesses you have to make that conclusion? Please show detailed steps.

(1) Let $p = 113$. For *k* primality witnesses of *p* the probability that *p* is composite is at most $1/2^k$ under Fermat's primality test.
(2) Checking the first 10 prime numbers 2, 3, 5, 7, 11, 13, 17, 19, 23 and 29
  (a) $2^{112} \equiv 1\, mod\, 113$
  (b) $3^{112} \equiv 1\, mod\, 113$
  (c) $5^{112} \equiv 1\, mod\, 113$
  (d) $7^{112} \equiv 1\, mod\, 113$
  (e) $11^{112} \equiv 1\, mod\, 113$
  (f) $13^{112} \equiv 1\, mod\, 113$
  (g) $17^{112} \equiv 1\, mod\, 113$
  (h) $19^{112} \equiv 1\, mod\, 113$
  (i) $23^{112} \equiv 1\, mod\, 113$
  (j) $29^{112} \equiv 1\, mod\, 113$
(3) After checking 10 witnesses we conclude that the number 113 is prime with a probability of $1/2^{10} = 99.90234375\%$

Checking again for another “random” number.

(4) Let $p = 561$. For *k* primality witnesses of *p* the probability that *p* is composite is at most $1/2^k$ under Fermat's primality test.
(5) Checking the first 10 prime numbers 2, 3, 5, 7, 11, 13, 17, 19, 23 and 29
  (a) $2^{560} \equiv 1\, mod\, 561$
  (b) $3^{560} \not\equiv 1\, mod\, 561$
(6) After checking 2 witnesses we conclude that the number 561 is composite.

7 Finite Field Representation (10%)

Please construct additive and multiplicative representation of a field GF(2^3) using irreducible polynomial x^3 + x + 1.

MUL	ADD	INT
0	0	0
x^0	1	1
x^1	x	2
x^2	x^2	4
x^3	x^2+1	5
x^4	x^2+x+1	7
x^5	x+1	3
x^6	x^2+x	6

F(X) = x^3+x+1

F(0) = 0 + 0 + 1 = 1
F(x^0) = x^0 + x^0 + 1 = 1
F(x) = x5 + x + 1 = x + 1 + x + 1 = 0
F(x^2) = x^10 + x^2 + 1 = x^3 + x^2 + 1 = x^2 + 1 + x^2 + 1 = 0
F(x^3) = x^15 + x^3 + 1 = x + x^2 + 1 + 1 = x^2 + x
F(x^4) = x^20 + x^4 + 1 = x^2 + x + x^2 + x + 1 + 1 = 0
F(x^5) = x^25 + x^5 + 1 = x^2 + x + 1 + x + 1 + 1 = x^2 + 1
F(x^6) = x^30 + x^6 + 1 = x^2 + x^2 + x + 1 = x + 1

Please construct a finite field GF(2^4) using polynomial x^4 + x + 1.

MUL	ADD	INT
0	0	0
x^0	1	1
x^1	x	2
x^2	x^2	4
x^3	x^2+1	5
x^4	x^2+x+1	7
x^5	x+1	3

x^6	x^2+x	6

F(X) = x^4+x+1

F(0) = 0 + 0 + 1 = 1
F(x^0) = x^0 + x^0 + 1 = 1
F(x) = x5 + x + 1 = x + 1 + x + 1 = 0
F(x^2) = x^10 + x^2 + 1 = x^3 + x^2 + 1 = x^2 + 1 + x^2 + 1 = 0
F(x^3) = x^15 + x^3 + 1 = x + x^2 + 1 + 1 = x^2 + x
F(x^4) = x^20 + x^4 + 1 = x^2 + x + x^2 + x + 1 + 1 = 0
F(x^5) = x^25 + x^5 + 1 = x^2 + x + 1 + x + 1 + 1 = x^2 + 1
F(x^6) = x^30 + x^6 + 1 = x^2 + x^2 + x + 1 = x + 1

8 Groups and Cosets (10%)

Assume G is a cyclic group of order 20 with generator a.
(1) What are the orders (individually) of a^3, a64, and a^14? Note that the notation ax refers to the element of a group.
By Lagrange's theorem, the order of any subgroup of G divides 20. We thus need to check if g^k = e for $k \in \{2, 4, 5, 10, 20\}$ and $g = \{a^3, a^4, a^{14}\}$, where e = a^0 is the identity of G.

$g = a^3$ we have $(a^3)^2 = a^6 != e$, $(a^3)^4 = a^{12} != e$, $(a^3)^5 = a^{15} != e$ and $(a^3)^{10} = a^{30} = a^{2*10+10} = a^{10} != e$ By exclusion, the order of a^3 must be 20 (it generates the whole group G).
$g = a^4$ we have $(a^4)^5 = a^{20} = e$ and 5 is the smallest divisor such that this condition holds (since (a^4)^2 = a^8 and (a^4)^4 = a^16). Hence the order of a^4 is 5.
$g = a^{14}$ we have $(a^{14})^{10} = a^{140} = a^{20*7} = e$, and 10 is the smallest divisor such that this condition holds. Thus the order of a^14 is 10.

(2) How many distinct cosets are there of H = <a^5>?
We consider only the number of left cosets (the number of right cosets is the same). The element a^5 has order 4, since (a^5)^4 = a^20 = e and this is the smallest divisor for which this condition is verified. Thus, the subgroup H is composed of 4 elements. Since the distinct cosets of H forms a partition of G, and each coset is composed of 4 elements (because we are just multiplying an element $g \in G$ with each element $h \in H$, and such mapping is injective), it follows that there are 20/4 = 5 distinct cosets of H.

(3) How many distinct cosets are there of H = <a^7>?

9S-box Calculation (20%)

(1) Show additive, multiplicative, and vector representation of field elements. And show the truth table for this S-Box. Use irreducible polynomial x3 + x + 1 and b = 2.

MLT	ADD	VEC	INT
0	0	000	0
α^0	1	001	1
α^1	α	010	2
α^2	α^2	100	4
α^3	$\alpha + 1$	011	3
α^4	$\alpha^2 + \alpha$	110	6
α^5	$\alpha^2 + \alpha + 1$	111	7
α^6	$\alpha^2 + 1$	101	5

Because $x^{-1}$is the same to x^6due to Fermat's Little Theorem and see that b=2 correlates with α in additive notation.

x	$x + 1$	$(x + 1)^2$	x^6	$(x + 1)^2 * x^6$	$(x + 1)^2 * x^6 + \alpha$
0	1	1	0	0	α
1	0	0	α^0	0	α
α	$\alpha + 1$	α^6	α^6	α^5	$\alpha^2 + 1$
$\alpha + 1$	α	α^2	α^{18}	α^6	$\alpha^2 + \alpha + 1$
α^2	$\alpha^2 + 1$	α^{12}	α^{12}	α^3	1
$\alpha^2 + 1$	α^2	α^4	α^{36}	α^5	$\alpha^2 + 1$
$\alpha^2 + \alpha$	$\alpha^2 + \alpha + 1$	α^{10}	α^{24}	α^6	$\alpha^2 + \alpha + 1$

$\alpha^2 + \alpha + 1$	$\alpha^2 + \alpha$	α^8	α^{30}	α^3	1

So, the S-box truth table is 2,2,5,7,1,5,7,1

(2) What is the nonlinearity based on the calculated Walsh-Hadamard value? Assume this is the maximal value in the Walsh-Hadamard spectrum.
Calculating the Walsh-Hadamard spectrum for v=011 and a=011

For v=011 we combine the last two coordinates and obtain the Boolean function 1,1,1,0,1,1,0,1.
$W_f(011) = (-1)^{1\oplus 0*3} + (-1)^{1\oplus 1*3} + (-1)^{1\oplus 2*3} + (-1)^{0\oplus 3*3} + (-1)^{1\oplus 4*3} + (-1)^{1\oplus 5*3} + (-1)^{0\oplus 6*3} + (-1)^{1\oplus 7*3}$
$W_f(011) =- 1 + 1 + 1 + 1 + 1 + 1 - 1 + 1 = 4$

Nonlinearity equals 2 since $2^{n-1} - 1/2|W_{max}|$