Homework 2a

Jacob Doskocil

October 9th, 2018

1. Prove that

   (a) $a \equiv b \mod n \implies b \equiv a \mod n$

   Proof. Assume $a \equiv b \mod n$
   $a \equiv b \mod n \implies a = b + k \times n$ where k is an integer
   so $a - b = k \times n$
   This also means that $b - a = -k \times n$ where $-k$ is also an integer.
   This means that $b = a + (-k) \times n$
   $\therefore b \equiv a \mod n$ □

   (b) $a \equiv b \mod n$ and $b \equiv c \mod n \implies a \equiv c \mod n$

   Proof. Assume $a \equiv b \mod n$ and $b \equiv c \mod n$
   $a = b + k \times n$ and $b = c + m \times n$
   Substituting the second equation for b into the first equation gives
   $a = (c + m \times n) + k \times n$
   Which can be rewritten as
   $a = c + (m + k) \times n$
   Since m is an integer and k is an integer, $(m + k)$ is also an integer.
   $\therefore$a $\equiv c \mod n$ □

2. Using extended Euclidean algorithm find the multiplicative inverse of

   (a) $1234 \mod 4321$
   1082

   (b) $24140 \mod 40902$
   is not invertable. $710 \times 24140 + 1203 \times 40902 = 0$

   (c) $550 \mod 17969$
   2581

   Extended Euclidean Algorithm means
   $m \times a + k \times n = 1$
   Start with with $k = m = 1$ and increase the one whose product is less, until the two products have a difference of 1. Using this method, the resulting m is the inverse. If the sum is ever 0, the value is not invertable, as $\gcd(a, n) \neq 1$. The above problems were solved using the program in the repository called `invert.cpp`

3. Determine which of the following are reducible over GF(2)

   (a) $x^3 + 1$
   $(x+1)(x^2+x+1) = x^3 + 2x^2 + 2x + 1 \equiv x^3 + 1 \mod 2$

   (b) $x^3 + x^2 + 1$
   This polynomial is irreducible over GF(2).

   (c) $x^4 + 1$
   $(x^2+1)(x^2+1) = x^4 + 2x^2 + 1 \equiv x^4 + 1 \mod 2$

4. Determine the GCD of following pair of polynomials:

   (a) $x^3 - x + 1$ and $x^2 + 1$ over GF(2)
   To solve this the polynomials must be factored into irreducible polynomials. $x^3 - x + 1 \equiv x^3 + x + 1$ which is irreducible over GF(2). $x^2 + 1 \equiv x^2 + 2x + 1 \mod 2$, which factors into $(x+1)(x+1)$. There are no irreducible factors in common, so the GCD is 1.

   (b) $x^5 + x^4 + x^3 - x^2 - x + 1$ and $x^3 + x^2 + x + 1$ over GF(3)
   This problem is solved the same way. $x^5 + x^4 + x^3 - x^2 - x + 1 \equiv x^5 + x^4 + 2x^2 + 2x + 1 \mod 3$ which factors into $(x+1)(x^4+x^2+x+1)$. x^3+x^2+x+1 factors into $(x+1)(x^2+1)$. The product of all the common factors is the GCD, which in this case is $(x+1)$.

5. For a cryptosystem $\{P, K, C, E, D\}$ where
   $P = \{a, b, c\}$ with
   $P_P(a) = \frac{1}{4}$, $P_P(b) = \frac{1}{4}$, $P_P(c) = \frac{1}{2}$

   $K = \{k1, k2, k3\}$ with
   $P_K(k1) = \frac{1}{2}$, $P_K(k2) = \frac{1}{4}$, $P_K(k3) = \frac{1}{4}$

   $C = \{1, 2, 3, 4\}$

$E_k(P)$	a	b	c
$k1$	1	2	1
$k2$	2	3	1
$k3$	3	2	4
$k4$	3	4	4

   Calculate $H(K|C)$
   First we can calculate the total probabilities of every combination of key and message where $P(K \cap P) = P_K(K) \times P_P(P)$. The table below on the left shows the probabilities. This table, as well as the given table of outputs for given keys and messages can be used to find the probability of a certain key and cryptotext, shown in the table on the right.

$P(K \cap P)$	a	b	c
$k1$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{4}$
$k2$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{8}$
$k3$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{8}$
$k4$	0	0	0

$P(K \cap C)$	1	2	3	4
$k1$	$\frac{3}{8}$	$\frac{1}{8}$	0	0
$k2$	$\frac{1}{8}$	$\frac{1}{16}$	$\frac{1}{16}$	0
$k3$	0	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{8}$
$k4$	0	0	0	0

The columns of the table on the right can be added up to give:
$P_C(1) = \frac{1}{2}$, $P_C(2) = \frac{1}{4}$, $P_C(3) = \frac{1}{8}$, $P_C(4) = \frac{1}{8}$
Finally this can be used to calculate the values of $P(K|C)$ using the formula $P(A \cap B) = P(A|B) \times P(B)$. The solution can be found in the table below.

$H(K\|C)$	1	2	3	4
$k1$	$\frac{3}{4}$	$\frac{1}{2}$	0	0
$k2$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{2}$	0
$k3$	0	$\frac{1}{4}$	$\frac{1}{2}$	1
$k4$	0	0	0	0