QUIZ 4 : MATH/CSE 4161

MARCH 6, 2012

$P(w=AC \mid \text{second letter } C) = \frac{P(w=AC \ \& \ \text{second letter } C)}{P(\text{second letter } C)} = \frac{5/10 \cdot 2/10}{5/10 \cdot 2/10 + 1/10 \cdot 2/10 + 4/10 \cdot 1/10} = \frac{10}{16}$

OPEN BOOK, OPEN NOTES, OPEN CALCULATOR, CLOSED FRIENDS AND ENEMIES

(1) A computer program generates words by choosing the first letter from the frequency table at the left and each additional letter is chosen using the table of conditional biletter frequencies at the right.
   (a) How much information is learned on average when you are told the output of a two letter word produced by this program given that you know the first letter is an A?
   (b) How much information is learned on average when you are told the output of a two letter word produced by this program given that you know the second letter is C? $\frac{10}{16}\log_2 16/10 + \frac{6}{16}\log_2 16/2 + \frac{4}{16}\log_2 16/4$
   (c) How much information is learned on average when you are told the output of a three letter word produced by this program given that you know that all three of the letters are the same?

$P(w=AC \mid \text{second letter } C)$
$P(w=BC \mid \text{second letter } C)$
$P(w=CC \mid \text{second letter } C)$

A	5
B	1
C	4

	A	B	C
A	5	3	2
B	1	7	2
C	3	6	1

(2) Let X and Y be random variables representing the outcomes of rolling 6 sided dice. How much information is learned on average when you are told the outcome of the difference of these rolls? That is, what is $H(|X - Y|)$?

(3) Say you have 8 coins and one of them is heavier than the other 7, but you can't tell by looking at it or just by touch. Say that you do however have a balance scale which if you weigh coins against each other and will tell you if the left pan is heavy, right pan is heavy or both pans are equal.
   (a) If the location of the heavier coin is a random event, how much information is learned on average when you are told which coin is heavier?
   (b) If you really do gain $log_2(3) \approx 1.58$ bits of information per weighing, what is the maximum number of weighings that you should need to determine which of the 8 coins is the heavy one? Explain why (write a sentence!).
   (c) Draw a decision tree which demonstrates that it is possible to determine which of the coins is heavy in this number of weighings.
   (d) Say that you weigh coins 1 and 2 vs. 3 and 4 on your first weighing. How much information do you learn on average from that particular weighing?

(4) Say that you have three plaintexts $\{m_1, m_2, m_3\}$ with respective probability 1/6, 1/3 and 1/2. Also say that you have four keys $\{k_1, k_2, k_3, k_4\}$ which are equally likely. Does the system achieve perfect secrecy? Why or why not (write a sentence!)?

	k_1	k_2	k_3	k_4
m_1	c_4	c_2	c_1	c_3
m_2	c_3	c_2	c_4	c_1
m_3	c_2	c_1	c_3	c_4

Computational elements that we will use in some new cryptosystems

- Compute $a^k \ (mod\ m)$ using only squaring operations and multiplication by a. ✓
- $gcd(a, b)$ using the Euclidean algorithm ✓
- Find k and ℓ such that

$$ka + \ell b = gcd(a, b) \quad \checkmark$$

- If $gcd(a, m) = 1$, then there is a k such that

$$ak \equiv 1 \ (mod\ m) \quad \checkmark$$

find k & ℓ s.t. $k \cdot a + \ell \cdot m = 1$
then $k \cdot a \equiv 1 \pmod m$

definition $ak \equiv 1 \pmod m \iff ak - 1 = -\ell \cdot m$ for some $\ell \in \mathbb{Z}$

There is a function called the Euler 'phi' function

$\phi(n) = \#$ of integers relatively prime (i.e. $gcd(k, n) = 1$) and are between 1 and n

n	integers between 1 and n which are relatively prime	$\phi(n)$
1	1	1
2	1	1 ✓
3	1,2	2 ✓
4	1,3	$2 = 2^2 - 2^1 = 4 - 2$ ✓
5	1,2,3,4	4 ✓
6	1,5	$2 = \phi(2) \cdot \phi(3) = (2-1)(3-1)$
7	1,2,3,4,5,6	6 ✓
8	1,3,5,7	$4 = 2^3 - 2^2 = 8 - 4$ ✓
9	1,2,4,5,7,8	$6 = 3^2 - 3 = 9 - 3$ ✓
10	1,3,7,9	$4 = \phi(5) \cdot \phi(2) = (5-1)(2-1) = 4$
11	1,2,3,4,5,6,7,8,9,10	10 ✓
12	1,5,7,11	$4 = \phi(4)\phi(3) = 2 \cdot 2 = 4$
14	1,3,5,9,11,13	$6 = \phi(7)\phi(2) = (7-1)(2-1)$

$\phi(n)$ = # of integers in $[1, n]$ which have gcd with $n = 1$

Let $[a, b]$ represent the interval of integers $\{a, a+1, \ldots, b-1, b\}$.

Notice that if p is prime

$\phi(p)$ = # of integers in [1,p] that have common factor with p

$= p - 1$

Also, $[1, 3^5]$ $\{3, 6, 9, 12, \ldots, 3^5 - 3, 3^5\}$ have a common factor with 3^5 $\phi(3^5) = 3^5 - 3^5/3$

$\phi(p^k) = p^k -$ # of integers in $[1,p^k]$ divisible by p

$= p^k -$ # of $r \cdot p$ where $1 \le r \le p^{k-1}$

$= p^k - p^{k-1}$

$1, \cancel{2}, \cancel{3}, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, \cancel{9}, \cancel{10}, 11$

$\phi(12) = 4$

$$\phi(p^k \cdot n) = (p^k - p^{k-1}) \cdot \phi(n) \quad \text{if } \gcd(n, p) = 1$$

Say that p does not divide n. Then let h be the number of integers in $[1, n]$ that have a common factor with n.

$\phi(p^k n) = np^k -$ # of integers in $[1,np^k]$ with a common factor with n or p (# int in $[1, n \cdot p^k]$)

$= np^k -$ # in $[1,np^k]$ with a common factor with n

$-$ # in $[1,np^k]$ with a common factor with p

$+$ # in $[1,np^k]$ with a factor with both n and p

$= np^k - hp^k - np^{k-1} + hp^{k-1}$ $[1, 2, 3, \ldots, p, p+1, p+2, \ldots, np^k]$

$= (n - h)(p^k - p^{k-1}) = \phi(n)(p^k - p^{k-1}) = \phi(n) \cdot \phi(p^k)$

divisible by p & have a common factor with n

if $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ where p_i are all distinct primes, then

$$\phi(n) = (p_1^{a_1} - p_1^{a_1 - 1})(p_2^{a_2} - p_2^{a_2 - 1}) \cdots (p_k^{a_k} - p_k^{a_k - k})$$

Example $m = 12$ $\phi(12) = 4$

$a = 5$ $\gcd(5, 12) = 1$

$$5^4 \equiv 1 \pmod{12}$$

$$5^2 \equiv 25 \equiv 1 \pmod{12}$$

$$5^4 \equiv 25^2 \equiv 1^2 \equiv 1 \pmod{12}$$

$m =$

Exercises:

1. Compute $\phi(50910363)$ knowing that

$$50910363 = 3^4 \times 7^2 \times 101 \times 127.$$

2. Use your answer from the previous question to compute

$$2^{28576807} \ mod \ 50910363.$$

3. Compute 3^{999} mod 143.

$143 = 13 \cdot 11$ $\quad \phi(143) = (13-1)(11-1)$

$= 12 \cdot 10 = 120$

$3^{999} \equiv (3^{120})^8 \cdot 3^{39} \pmod{143}$ $\quad 8 \cdot 120 = 960$

$\equiv 3^{39} \pmod{143}$

$126 \equiv -17 \pmod{143}$

$3^2 \equiv 9$

$3^4 \equiv 81$

$3^8 \equiv 81^2 \equiv 126 \pmod{143}$

$3^{16} \equiv (-17)^2 \equiv 3$

$3^{32} \equiv 9$

$3^{39} \equiv 3^{32} \cdot 3^4 \cdot 3^2 \cdot 3^1$

$\equiv 3^2 \cdot 3^4 \cdot 3^2 \cdot 3^1$

$\equiv 3^9 \equiv 126 \pmod{143}$

4
17
17
119
17
289

1
126
3
378

5
41
143 | 561
572
841
715
126