HW 11 CMSC 456. MORALLY DUE Dec 3
SOLUTIONS
NOTE- THE HW IS FIVE LONG

1. (0 points) READ the syllabus- Content and Policy. What is your name? Write it clearly. What is the day of the final? READ the slides and notes on Perfect and Comp Secrecy.

GOTO NEXT PAGE

2. (30 points) In this problem we will guide you through a proof that a bad random string generator will result in a 1-time pad that is NOT secure in that Eve has prob $> \frac{1}{2}$ of winning the security game.

   Alice and Bob are using a 1-time pad. But their random bit generator is terrible! It outputs 0^n with probability $\frac{1}{2} + \frac{1}{2^{n+1}}$, and every other string of length n with probability $\frac{1}{2^{n+1}}$. Answer the following questions which will lead up to a proof that Alice and Bob's 1-time pad leads to an insecure cipher. You can assume n is odd and large.

   (a) (0 points) Eve picks $m_0 = 0^n$ and $m_1 = 1^n$.

   (b) (3 points) What is $\Pr(m = m_0)$? $\Pr(m = m_1)$?

   (c) (0 points) Recall that Alice picks $m \in \{m_0, m_1\}$ and then generates the key k (very badly!) and sends Eve $c = m \oplus k$.

   (d) (0 points) Let MAJ0 be the event: *c is over half 0's.* Let MAJ1 be the event: *c is over half 1's.*. We will take n odd so that either MAJ0 or MAJ1 occurs.

   (e) (3 points) What is $\Pr(MAJ0|m = m_0)$? (Do not use the definition of Cond Prob- use instead that IF $m = m_0$, what is the prob that the key k is such that $c = m \oplus k$ has majority 0's.) (You can approximate by taking $\frac{1}{2^{n+1}}$ to be 0. We are assuming n is large.)

   (f) (3 points) What is $\Pr(MAJ1|m = m_1)$? (Do not use the definition of Cond Prob- use instead that IF $m = m_1$, what is the prob that the key k is such that $c = m \oplus k$ has majority 1's.) (You can approximate by taking $\frac{1}{2^{n+1}}$ to be 0. We are assuming n is large.)

   (g) (3 points) What is $\Pr(MAJ0|m = m_1)$? (Do not use the definition of Cond Prob- use instead that IF $m = m_1$, what is the prob that the key k is such that $c = m \oplus k$ has majority 0's.) (You can approximate by taking $\frac{1}{2^{n+1}}$ to be 0. We are assuming n is large.)

   (h) (3 points) What is $\Pr(MAJ1|m = m_0)$? (Do not use the definition of Cond Prob- use instead that IF $m = m_0$, what is the prob that the key k is such that $c = m \oplus k$ has majority 1's.) (You an approx by taking $\frac{1}{2^{n+1}}$ to be 0. We are assuming n is large.)

GOTO NEXT PAGE FOR MORE OF THIS PROBLEM

(i) (3 points) What is $\Pr(MAJ0)$? (Hint: its

$$\Pr(MAJ0|m = m_0)\Pr(m = m_0) + \Pr(MAJ0|m = m_1)\Pr(m = m_1)$$

and you have all of those parts.)

(j) (3 points) What is $\Pr(MAJ1)$? (Hint: its

$$\Pr(MAJ1|m = m_0)\Pr(m = m_0) + \Pr(MAJ1|m = m_1)\Pr(m = m_1)$$

and you have all of those parts.)

(k) (3 points) What is $\Pr(m = m_0|MAJ0)$ (Hint: Use Bayes's theorem)

(l) (3 points) What is $\Pr(m = m_1|MAJ1)$ (Hint: Use Bayes's theorem)

(m) (3 points) Show that Eve has a winning strategy. Describe the strategy and use the parts above to show it has prob $> \frac{1}{2}$ of winning. What is the prob of Eve winning?

SOLUTION TO PROBLEM TWO

(a) (0 points) Eve picks $m_0 = 0^n$ and $m_1 = 1^n$.

(b) (3 points) What is $\Pr(m = m_0)$? $\Pr(m = m_1)$?
ANSWER: Both are $\frac{1}{2}$ since Alice picks them by flipping a fair coin.

(c) (0 points) Recall that Alice picks $m \in \{m_0, m_1\}$ and then generates the key k (very badly!) and sends Eve $c = m \oplus k$.

(d) (0 points) Let MAJ0 be that c is over half 0's. R-O Let MAJ1 be that c is over half 1's. (We will take n odd so that either MAJ0 or MAJ1 occurs).

(e) (3 points) What is $\Pr(MAJ0|m = m_0)$? (Do not use the definition of Cond Prob- use instead that IF $m = m_0$, what is the prob that the key is such that $c \oplus k$ has majority 0's.) (You an approx by taking $\frac{1}{2^{n+1}}$ to be 0. We are assuming n is large.)

(f) ANSWER: $\Pr(MAJ0|m = 0^n)$: If $m = 0^n$ then there are several ways that $MAJ0$ could happen:

- $k = 0^n$. This happens with prob $\frac{1}{2} + \frac{1}{2^{n+1}}$.
- k is not 0^n but has over half 0's. Since n is large we can take this to be approx $\frac{1}{4}$.

Hence $\Pr(MAJ0|m = 0^n) \sim \frac{3}{4} + \frac{1}{2^{n+1}} \sim \frac{3}{4}$.

(3 points) What is $\Pr(MAJ1|m = m_1)$? (Do not use the definition of Cond Prob- use instead that IF $m = m_1$, what is the prob that the key is such that $c \oplus k$ has majority 1's.) (You an approx by taking $\frac{1}{2^{n+1}}$ to be 0. We are assuming n is large.)

ANSWER: Similar to the last part, answer is $\frac{3}{4}$.

(g) (3 points) What is $\Pr(MAJ0|m = m_1)$? (Do not use the definition of Cond Prob- use instead that IF $m = m_1$, what is the prob that the key is such that $c \oplus k$ has majority 0's.) (You an approx by taking $\frac{1}{2^{n+1}}$ to be 0. We are assuming n is large.)

ANSWER: Similar to the last part, answer is $\frac{1}{4}$.

(h) (3 points) What is $\Pr(MAJ1|m = m_0)$? (Do not use the definition of Cond Prob- use instead that IF $m = m_0$, what is the prob that the key is such that $c \oplus k$ has majority 1's.) (You an approx by taking $\frac{1}{2^{n+1}}$ to be 0. We are assuming n is large.)

ANSWER: Similar to the last part, answer is $\frac{1}{4}$.

(i) (3 points) What is $\Pr(MAJ0)$? (Hint: its $\Pr(MAJ0|m = m_0)\Pr(m = m_0) + \Pr(MAJ0|m = m_1)\Pr(m = m_1)$ and you have all of those parts.)

ANSWER: $\frac{3}{4}\frac{1}{2} + \frac{1}{4}\frac{1}{2} = \frac{1}{2}$

(j) (3 points) What is $\Pr(MAJ1)$? (Hint: its $\Pr(MAJ1|m = m_0)\Pr(m = m_0) + \Pr(MAJ1|m = m_1)\Pr(m = m_1)$ and you have all of those parts.)

ANSWER: Similar to above, its $\frac{1}{2}$.

(k) (3 points) What is $\Pr(m = m_0|MAJ0)$ (Hint: Use Bayes's theorem)

ANSWER:

$$\Pr(m = m_0|MAJ0) = \Pr(MAJ0|m = m_0)\frac{\Pr(m = m_0)}{\Pr(MAJ0)} = \frac{\frac{3}{4}\frac{1}{2}}{\frac{1}{2}} = \frac{3}{4}$$

(l) (3 points) What is $\Pr(m = m_1 | MAJ1)$ (Hint: Use Bayes's theorem)

ANSWER: Similar to the above. $\frac{3}{4}$.

(m) (3 points) Show that Eve has a winning strategy. Describe the strategy and use the parts above to show it has prob $> \frac{1}{2}$ of winning. What is the prob of Eve winning?

ANSWER: Eve's strategy: look at c. If it has more 0's than 1's then guess $m = 0^n$. If it has more 1's then 0's then guess $m = 1^n$. By the above this wins with prob $\frac{3}{4}$.

END OF SOLUTION TO PROBLEM TWO
GOTO NEXT PAGE

3. (30 points) In this problem we will make what we said about the Randomized Shift rigorous lay the groundwork for being able to apply the technique elsewhere.

   (a) (10 points) (Look up THE BIRTHDAY PARADOX on the web though you will need to adjust it some.) Find a number a such that, for large N, $a\sqrt{N}$ elements from $\{1,\ldots,N\}$ with replacement then the probability that two are the same is $\geq \frac{3}{4}$ (the traditional birthday Paradox is $\frac{1}{2}$ so you will need to adjust this.) You have to hand in a self-contained account, you can't say *see website BLAH.*

   (b) (10 points) Assume you are doing randomized shift with an alphabet of size N. Show that the randomized shift is not computationally secure by giving a strategy in the comp sec game where Eve wins with prob much bigger than $\frac{1}{2}$. (You may use part 1 above.)

   (c) (10 points) Assume the alphabet size N is prime. Hence the number of (a,b) such that $ax+b$ is a valid Affine Cipher is N^2 (we will not let $b=0$). Recall the RANDOMIZED AFFINE CIPHER:

      i. Alice and Bob both have the key which is a function $f : \{1,\ldots,N^2\} \to \{1,\ldots,N\} \times \{1,\ldots,N\}$.

      ii. For Alice to send Bob a message $\sigma_1,\sigma_2,\ldots,\sigma_L$ he (1) generates RANDOM $r_1,\ldots,r_L \in \{1,\ldots,N^2\}$, (2) for $1 \leq i \leq L$ Alice finds $f(r_i)=(a_i,b_i)$. (3) sends

      $$(r_1, a_1\sigma_1+b_1), (r_2, a_2\sigma_2+b_2), \ldots, (r_L, a_L\sigma_L+b_L)$$

      iii. We leave it to you for how Bob decodes, but note that since he has r_i's he can find a_i's and b_i's.

   Show that the randomized affine is not computationally secure by giving a strategy in the comp sec game where Eve wins with prob much bigger than $\frac{1}{2}$. (You may need to reason a bit informally towards the end of the proof.)

SOLUTION TO PROBLEM THREE

1) Prob that they are all different is

$$\frac{N}{N}\frac{N-1}{N}\cdots\frac{N-M}{N} = (1-\frac{1}{N})(1-\frac{2}{N})\cdots(1-\frac{M}{N})$$

$\sim e^{(-1-2-3-\cdots-M)/N} = e^{M^2/2}$

So need $e^-M^2 2N \le \frac{1}{4}$

$-M^2/2N \le \ln((1/4) = -1.38$

$-M^2/N \le -2.76$

$2.76 \le M^2/N$

$2.76N \le M^2$

$M \ge \sqrt{2.76N} = 1.66\sqrt{N}.$

2) Let the alphabet be $\{\sigma_1, \ldots, \sigma_N\}$.
Let $m_0 = \sigma_1^M$ where we will determine M later, and $m_1 = \sigma_1\sigma_2\cdots\sigma_M$.
The r_i's will be from $\{\sigma_1, \ldots, \sigma_N\}$. Hence if we take $a\sqrt{N}$ of them then we are likely to get two r's that are the same.
So we let $M = s\sqrt{N}$ (rounded up).

3) Let the alphabet be $\{\sigma_1, \ldots, \sigma_N\}$.
Let

$$m_0 = \sigma_1^{2N}$$

and

$$m_1 = \sigma_1\sigma_2\cdots\sigma_N\sigma_1\sigma_2\cdots\sigma_N.$$

Eve sees ciphertext

$$(r_1, \tau_1)\cdots(r_{2N}, \tau_{2N})$$

The r_i's come from N^2 possibilities. Since we have $2N > 1.66\sqrt{N^2}$ the prob is $\ge \frac{3}{4}$ that there are two r_i's that are the same.
So there exists $1 \le i < j \le 2N$ such that $r_i = r_j$.

If $\tau_i \neq \tau_j$ then we KNOW that the string was m_1.

If $\tau_i = \tau_j$ and $i \not\equiv j \pmod{N}$ then we KNOW the string is m_0

If $\tau_i = \tau_j$ and $i \equiv j \pmod{N}$ then we note this is unlikely so we can just guess and not worry about the probability.

END OF SOLUTION TO PROBLEM THREE

GOTO NEXT PAGE

4. (40 points) State two facts you learned from Lloyd's talk on the NSA.