hw11 Solutions

hw11 Problem 2: An Imperfect Random Generator Makes 1-Time Pad Insecure

Problem 2

Alice and Bob are using a 1-time pad.

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.

Problem 2:a,b,c,d,e

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

b) 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) Recall that Alice picks $m \in \{m_0, m_1\}$ and then generates k (badly!) and sends Eve $m \oplus k$.

d) Let MAJ0 be that c is over half 0's.

e) Let MAJ1 be that c is over half 1's.

Problem 2: f,g,h,i

f) What is $\Pr(MAJ0|m = m_0)$? (Approx $\frac{1}{2^{n+1}} \sim 0.$).)
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 $\Pr(MAJ0|m = 0^n) \sim \frac{3}{4} + \frac{1}{2^{n+1}} \sim \frac{3}{4}$.

g) What is $\Pr(MAJ1|m = m_1)$? ANSWER: Similar to above, $\frac{3}{4}$.

h) What is $\Pr(MAJ0|m = m_1)$? ANSWER: Similar to above, $\frac{1}{4}$.

i) What is $\Pr(MAJ1|m = m_0)$? ANSWER: Similar to above, $\frac{1}{4}$.

Problem 2: j,k

j) What is $\Pr(MAJ0)$?
ANSWER: Its:

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

We have all of these parts so we get:

$$\frac{3}{4} \times \frac{1}{2} + \frac{1}{4} \times \frac{1}{2} = \frac{1}{2}$$

k) What is $\Pr(MAJ1)$? ANSWER: Similar to above, its $\frac{1}{2}$.

Problem 2: l,m

l) What is $\Pr(m = m_0|MAJ0)$ (Hint: Use Bayes's theorem)
ANSWER:

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

m) What is $\Pr(m = m_1|MAJ1)$ (Hint: Use Bayes's theorem)
ANSWER: Similar to the above. $\frac{3}{4}$.

Problem 2: n

n) 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 $\frac{3}{4}$.

Problem 3a: Problem and Solution

PROBLEM: Find a s.t., for large N, $a\sqrt{N}$ elts from $\{1,\ldots,N\}$ w/replacement then the prob that 2 same is $\geq \frac{3}{4}$

SOLUTION: Prob that they are all different is

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

Important! $1-z \sim e^{-z}$. Since N large $(1-\frac{c}{N}) \sim e^{-c/N}$. Hence: $\sim e^{(-1-2-3-\cdots-M)/N} = e^{-M^2/2N}$. So need $e^{-M^2/2N} \leq \frac{1}{4}$

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

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

$$2.76N \leq M^2$$

$$M \geq \sqrt{2.76N} = 1.66\sqrt{N} \text{ Take } a = 1.66$$

Problem 3b: Problem and Solution

PROBLEM: Rand shift, alphabet size N. Show not comp secure by giving a good strategy for Eve.

SOLUTION: Let the alphabet be $\{\sigma_1, \ldots, \sigma_N\}$.
Eve picks $m_0 = \sigma_1^M$, $m_1 = \sigma_1\sigma_2 \cdots \sigma_M$ where $M = a\sqrt{N}$.
Alice returns $(r_1, \sigma_1) \cdots (r_M, \sigma_M)$.
With prob $> \frac{3}{4}$ there will be $i < j$ with $r_i = r_j$. If that happens then Eve looks does the following:
If $\sigma_i = \sigma_j$ then m is m_0.
If $\sigma_i \neq \sigma_j$ then m is m_1.

Problem 3c: Problem

PROBLEM: Alphabet is size N, 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:

1. Alice and Bob both $f : \{1, \ldots, N^2\} \rightarrow \{1, \ldots, N\} \times \{1, \ldots, N\}$.
2. For Alice $\sigma_1, \sigma_2, \ldots, \sigma_L$ she (1) generates RANDOM $r_1, \ldots, r_L \in \{1, \ldots, N^2\}$, (2) for $1 \le i \le L$ Alice finds $f(r_i) = (a_i, b_i)$. (3) sends

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

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 $\frac{1}{2}$.

Problem 3c: Solution. First Attempt

SOLUTION: Let the alphabet be $\{\sigma_1, \ldots, \sigma_N\}$.
Eve: $m_0 = \sigma_1^M$, $m_1 = \sigma_1\sigma_2 \cdots \sigma_M$, M TBD.

Alice returns $(r_1, \sigma_1) \cdots (r_M, \sigma_M)$.

Eve WANTS there to be a repeat. There are N^2 possible r's so need $M = a\sqrt{N^2} = aN$. DOES NOT WORK since $a > 1$, and need $M \leq N$.
Start over again with new idea on next slide.

Problem 3c: Solution. Second Attempt

SOLUTION: Let the alphabet be $\{\sigma_1, \ldots, \sigma_N\}$.
Eve: $m_0 = \sigma_1^{2N}$, $m_1 = \sigma_1 \cdots \sigma_N \sigma_1 \cdots \sigma_N$.

Alice returns $(r_1, \sigma_1) \cdots (r_{2N}, \sigma_{2N})$.
Since $2N > aN$, with prob $> \frac{3}{4}$ there will be $i < j$ with $r_i = r_j$.
BUT: if $i \equiv j \pmod{N}$ then having $r_i = r_j$ won't help Eve!
However, the prob of that happening is small so we ignore it.
And now we can do the usual:
If $\sigma_i = \sigma_j$ then m is m_0.
If $\sigma_i \neq \sigma_j$ then m is m_1.

Problem 4

Name two things you learned from Lloyd's NSA talk?
Discuss!