Isaac Kim
CS 487
Professor Baldimtsi
Feb 4, 2023

Homework 1

2.

a) Expand Pr[M='now'|C='baa'] according to Bayes' Theorem:

$$\Pr[M\text{='now'}|C\text{='baa'}] = \frac{\Pr[C\text{='baa'}|M\text{='now'}]\cdot\Pr[M\text{='now'}]}{\Pr[C\text{='baa'}]}$$

Here, we could calculate Pr[C='baa'] and Pr[M='now'] separately, but note that the top of the fraction is 0, where Pr[C='baa'|M='now'] = 0 since there exists no key k, such that Enc_k('now') = 'baa' for the shift cipher. Anything multiplied by 0 is 0, and hence, **Pr[M='now'|C='baa'] = 0**.

b) Expand Pr[M='yes'|C='zft'] according to Bayes' Theorem:

$$\Pr[M\text{='yes'}|C\text{='zft'}] = \frac{\Pr[C\text{='zft'}|M\text{='yes'}]\cdot\Pr[M\text{='yes'}]}{\Pr[C\text{='zft'}]}$$

To find Pr[C='zft'], use law of total probability:

$$\Pr[C\text{='zft'}]=(\Pr[C\text{='zft'}|M\text{='yes'}]\cdot \Pr[M\text{='yes'}]) + (\Pr[C\text{='zft'}|M\text{='bye'}]\cdot \Pr[M\text{='bye'}]) + (\Pr[C\text{='zft'}|M\text{='now'}]\cdot \Pr[M\text{='now'}])$$

Note that Pr[C='zft'|M='bye']=0 and Pr[C='zft'|M='now']=0 since there exists no key k, such that Enc_k('now') = 'zft' or Enc_k('bye') = 'zft'. Then,

$$\Pr[C\text{='zft'}]=(\Pr[C\text{='zft'}|M\text{='yes'}]\cdot \Pr[M\text{='yes'}]) + (0\cdot \Pr[M\text{='bye'}]) + (0\cdot \Pr[M\text{='now'}])$$
$$\Pr[C\text{='zft'}]=\Pr[C\text{='zft'}|M\text{='yes'}]\cdot \Pr[M\text{='yes'}]$$

Pr[C='zft'|M='yes'] = $\frac{1}{26}$ since the only time this can occur is when k = 1, which has a probability of $\frac{1}{26}$. We know that Pr[M='yes']=0.5. Hence, Pr[C='zft']=$\frac{1}{26}$(0.5)
Then,

$$\Pr[M\text{='yes'}|C\text{='zft'}] = \frac{\Pr[C\text{='zft'}|M\text{='yes'}]\cdot\Pr[M\text{='yes'}]}{\Pr[C\text{='zft'}]}$$
$$\Pr[M\text{='yes'}|C\text{='zft'}] = \frac{\Pr[C\text{='zft'}|M\text{='yes'}]\cdot\Pr[M\text{='yes'}]}{\frac{1}{26}(0.5)}$$
$$\Pr[M\text{='yes'}|C\text{='zft'}] = \frac{\frac{1}{26}(0.5)}{\frac{1}{26}(0.5)}$$

Hence, **Pr[M='yes'|C='zft'] = 1**.

3.

a) Expand Pr[m='010'|c='010'] according to Bayes' Theorem:

$$\Pr[m\text{='010'}|c\text{='010'}] = \frac{\Pr[c\text{='010'}|m\text{='010'}]\cdot\Pr[m\text{='010'}]}{\Pr[c\text{='010'}]}$$

We know that Pr[c='010'] = 2^{-n}, and since $n = 3$, Pr[c='010'] = $\frac{1}{8}$. It was given that Pr[m='010'] = 0.5. Pr[c='010'|m='010'] = $\frac{1}{8}$ since this is equivalent to the probability that the key k = 000, which is $\frac{1}{8}$. Then,

$$\Pr[m=\text{'010'}|c=\text{'010'}] = \frac{\frac{1}{8}\cdot 0.5}{\frac{1}{8}} = 0.5$$

Hence, **Pr[$\boldsymbol{m}$='010'|$\boldsymbol{c}$='010'] = 0.5**.

b) This problem is identical to the 3a) except that m = '011'. Pr[m='011'] = 0.5, and Pr[c='010'|m='011'] = $\frac{1}{8}$ since this is equivalent to the probability that the key k = 001, which is $\frac{1}{8}$. Pr[c='010'] does not change. Then, by Bayes' Theorem:

$$\Pr[m=\text{'011'}|c=\text{'010'}] = \frac{\Pr[c=\text{'010'}|m=\text{'011'}]\cdot\Pr[m=\text{'011'}]}{\Pr[c=\text{'010'}]}$$
$$\Pr[m=\text{'010'}|c=\text{'010'}] = \frac{\frac{1}{8}\cdot 0.5}{\frac{1}{8}} = 0.5$$

Hence, **Pr[$\boldsymbol{m}$='011'|$\boldsymbol{c}$='010'] = 0.5**.

c) We know that an encryption scheme (Gen, Enc, Dec) with message space M and ciphertext space C is perfectly secret if for every distribution over M, for all $m_0, m_1 \in M$ and $c \in C$ with $\Pr[C = c] > 0$, it holds that:

$$\Pr[C = c|M = m_0] = \Pr[C = c|M = m_1]$$

To show that an encryption scheme is not secure, the opposite must hold true. Or, an encryption scheme with message space M and ciphertext space C is *not* perfectly secure if there exists a distribution over M such that for some $m_0, m_1 \in M$ and some $c \in C$ with $\Pr[C = c] > 0$,

$$\Pr[C = c|M = m_0] \neq \Pr[C = c|M = m_1]$$

If Alice decides to exclude the all zeroes key from her keyspace, then her encryption scheme becomes *not* perfectly secure. Let M be Alice's message space and C be Alice's ciphertext space. Also let $m \in M$ be Alice's original message and let $m_1 = m$ and $m_0 \in M$ be an arbitrary message, $m_0 \neq m_1$, and $c \in C$, $\Pr[C = c] > 0$.

Consider the ciphertext $c_0 \in C$ with $\Pr[C = c_0] > 0$, where $c_0 = Enc_{k_0}(m)$, $k_0 = 0^\lambda$. Then, since k_0 is omitted from our keyspace, for all keys k in our keyspace/$\{k_0\}$, $Enc_k(m) \neq c_0$. Then, $\Pr[C = c_0|M = m] = \Pr[C = c_0|M = m_1] = 0$. However, $\Pr[C = c_0|M = m_0] \neq 0$.

Hence, $\Pr[C = c_0|M = m_1] \neq Pr[C = c_0|M = m_0]$, and Alice's new encryption scheme is *not* perfectly secure!

d) Our new keyspace is now $k = (k_1, k_2), k_1, k_2 \in \{0,1\}^l$. Hence, there are $2^l \cdot 2^l = 2^{2l}$ keys in our new keyspace.

e) Since our encryption algorithm uses $c = k_1$ XOR (k_2 XOR m), we can generate keys such that 2 messages $m_0, m_1 \in M$ have the same ciphertext $c \in C$. Note that each key k in our new keyspace has an equal chance of being picked ($\frac{1}{l^2}$). The probability of generating a certain ciphertext $c \in C$ for m_0 is the same as generating the same ciphertext $c \in C$ for m_1. Hence, $\Pr[C = c|M = m_0] = Pr[C = c|M = m_1]$.

4. An attacker A will send two messages, m_0, m_1 to the challenger. The probability that A wins (the scenario where the attacker picks $b' = b$) is written as $\Pr[\text{Exp}_{A,\pi}(n) = 1]$. The Challenger picks $b = 0$ or $b = 1$ randomly to decide which message to encrypt, each with a probability of $\frac{1}{2}$. According to the law of total probability, we can rewrite $\Pr[\text{Exp}_{A,\pi}(n) = 1]$ as:

$$\Pr[\text{Exp}_{A,\pi}(n) = 1] = \Pr[\text{A picks } 0|b = 0] \cdot \tfrac{1}{2} + \Pr[\text{A picks } 1|b = 1] \cdot \tfrac{1}{2}$$

Consider an adversary that picks messages m_0 = 'aaaa', m_1 = 'aaab', $m_0, m_1 \in M, |M| = 4$. Given these messages and $|K| = 2$, for any key k, the second and last character of the ciphertext $c = Enc_k(m_0)$ will be the same, while the second and last character of $c = Enc_k(m_1)$ will be one apart. Then, the attacker will only have to look at these characters to distinguish which message was encrypted. Then:

Case 1 (b = 0): $\Pr[\text{A picks } 0|b = 0] = 1$

Case 2 (b = 1): $\Pr[\text{A picks } 1|b = 1] = 1$

In both cases, the attacker will know exactly which message was encrypted.

Then, $\Pr[\text{Exp}_{A,\pi}(n) = 1] = 1 \cdot \frac{1}{2} + 1 \cdot \frac{1}{2} = \frac{1}{2} + \frac{1}{2} = 1$ which is clearly not negligible ($\frac{1}{2} + \frac{1}{2} > \frac{1}{2} + \text{negl}(n)$, n is security parameter). Hence, the Vignerer cipher is not EAV-secure.

5. Let $G : \{0,1\}^n \to \{0,1\}^{2n}$ be a PRG for every n), and let $s \in \{0,1\}^n$. To show that the following constructions are not PRGs, we must show that either of these do not hold:

1. For every n, it holds that $l(n) > n$

OR

2. For any PPT algorithm D, there is a negligible function negl such that:

$$|\Pr[D(G_a(s)) = 1] - \Pr[D(r) = 1]| \leq \text{negl}(n)$$

where the first probability is taken over uniform choice of $s \in \{0,1\}^n$ and the randomness of D, and the second probability is taken over uniform choice of $f \in \{0,1\}^{l(n)}$ and the randomness of D.

a) Expansion factor $= 2n||2n = 4n > n$. This scenario is similar to what we did in lecture. The range for $G_a(s)$ consists of series of bits whose first half is identical to the second half. Let D be our distinguisher such that $D(w) = 1$ if and only if there exists an $s \in \{0,1\}^n$ such that $G_a(s) = w$ and let $r \in \{0,1\}^{4n}$. We must show that $|\Pr[D(G_a(s)) = 1] - \Pr[D(r) = 1]| \leq \text{negl}(n)$. Note that there are 2^{4n} possible strings under the uniform distribution $\{0,1\}^{4n}$, each having a probability of 2^{-4n} of being picked. The number of different strings in the range of $G_a(s)$ under uniform n-bit seed is 2^n. Therefore, the fraction of strings of length $4n$ that are in the range of G_a is at most $\frac{2^n}{2^{4n}} = 2^{-3n}$. Also note that most of the strings of length $4n$ have a probability of 0 being output by G_a. Then:

Case 1 ($G_a(s) = w$): $\Pr[D(G_a(s)) = 1] = 1$

Case 2 (w is taken from r over uniform choice and there exists an $s \in \{0,1\}^n$ such that $G_a(s) = w$): $\Pr[D(r) = 1] = 2^{-3n}$

Hence, $|\Pr[D(G_a(s)) = 1] - \Pr[D(r) = 1]| = 1 - 2^{-3n}$ which is clearly greater than negl(n).

b) Expansion factor $= 2n||2n = 4n > n$. Note that the latter half of $G_b(s)$ does not change. Then, the number of different strings in the range of $G_b(s)$ under uniform n-bit seed is 2^n. The range for $G_a(s)$ consists of series of bits whose first $2n$ bits is identical to $G(s)$, and the next $2n$ bits are $G(0^n)$. Let D be our distinguisher such that $D(w) = 1$ if and only if there exists an $s \in \{0,1\}^n$ such that $G_b(s) = w$ and let $r \in \{0,1\}^{4n}$. We must show that $|\Pr[D(G_b(s)) = 1] - \Pr[D(r) = 1]| \leq$negl($n$). There are 2^{4n} possible strings under the uniform distribution $\{0,1\}^{4n}$, each having a probability of 2^{-4n} of being picked. Therefore, the fraction of strings of length $4n$ that are in the range of G_b is at most $\frac{2^n}{2^{4n}} = 2^{-3n}$. Then:

Case 1 ($G_a(s) = w$): $\Pr[D(G_a(s)) = 1] = 1$

Case 2 (w is taken from r over uniform choice and there exists an $s \in \{0,1\}^n$ such that $G_b(s) = w$): $\Pr[D(r) = 1] = 2^{-3n}$

Hence, $|\Pr[D(G_a(s)) = 1] - \Pr[D(r) = 1]| = 1 - 2^{-3n}$ which is clearly greater than negl(n).