Math 441: Test I

Drew Blount

Monday, March 2

Problem 1 *The Zero Pad*

It is important to remember that, regardless of the choice of key (including Alice and Bob's unlikely 0^n), *the one-time pad is perfectly secure.* Thus, if any feasible eavesdropper of their message would be no stronger than the adversary in the adversarial indistinguishability experiment $\text{PrivK}^{eav}_{A,\Pi}$, Alice is correct. Say that Alice and Bob have message m, key $k = 0^n$ and ciphertext $c = m$. A $\text{PrivK}^{eav}_{A,\Pi}$ adversary, unaware of the encryption key, has no reason to discount the hypothesis that another message $m' \neq m$ was sent and encrypted with the key $k' = c \oplus m'$. This is precisely because the OTP is perfectly secure, because $Pr[C = c|M = m] = Pr[C = c|M = m']$.

It is easy to imagine a realistic scenario where an eavesdropper is not exactly the adversary in $\text{PrivK}^{eav}_{A,\Pi}$, however. Notably, if an eavesdropper is at prior (before eavesdropping) at all uncertain whether they will read an encrypted or unencrypted message, seeing something that looks like human speech (as Alice and Bob's message presumably does), will reasonably convince them that they are seeing something that was not padded by a random string. This is because the probability that a random-padded string looks like human speech is equal to the probability that a random string looks like human speech, which is obviously quite low. In other words, if you just happened across Alice and Bob's seemingly bare message, a reasonable person would probably assume that it was not padded by a random string. Then the naive attacker will interpret the message as unencrypted, which is bad news for Alice and Bob despite not being technically true.

I can't say that the perspective in the above paragraph is wholly unconvincing to me—in fact, if there is a non-negligible chance that such an attacker might see Alice and Bob's message, and if the cost of generating a new key and re-encrypting is negligible, Bob's advice is pragmatic and should be followed. This is a case of a back-door attack: if an adversary does not conform to the assumptions of $\text{PrivK}^{eav}_{A,\Pi}$, and is simply someone at prior uncertain of whether or not the message is encrypted, the encryption is not secure. However, as long as Alice and Bob are only up against people of the type of the adversary in $\text{PrivK}^{eav}_{A,\Pi}$, Alice is right.

In summary: choosing the zero key is no problem within the assumptions of $\text{PrivK}^{eav}_{A,\Pi}$—of course it isn't, because the OTP is perfectly secure. So within $\text{PrivK}^{eav}_{A,\Pi}$, Alice is right. Bob is the voice of our natural intuition here, which comes from a frame outside the strict assumptions of the $\text{PrivK}^{eav}_{A,\Pi}$ experiment.

. . . .

Problem 2 *Designing an Attack*

The scheme described in the problem statement can be broken by an adversary in the $\mathrm{PrivK}^{eav}_{A,\Pi}(n)$ experiment in this way:

1. Construct m_0 such that, when broken into blocks, the first block $m_{0,1}$ is an arbitrary string and the ith block $m_{0,i} = m_{0,i-1} - 1$. Choose m_1 to be an arbitrary string that does *not* have this "decrementing blocks" property.
2. When presented with the cipher text c, output 0 if c is the concatenation of identical blocks ($c_i = c_j$ for all i, j), 1 otherwise.

Now considering the fact that the function F_k is deterministic, and that under this scheme each $c_i = F_k(\mathrm{ctr} + i + m_i)$, you can see that for any *consecutive* block indices i, j,

$$\begin{aligned} c_{0,i} \equiv F_k(\mathrm{ctr} + i + m_{0,i}) = F_k(\mathrm{ctr} + j + m_{0,j}) \equiv c_{0,j} \\ c_{1,i} \equiv F_k(\mathrm{ctr} + i + m_{1,i}) \neq F_k(\mathrm{ctr} + j + m_{1,j}) \equiv c_{1,j} \end{aligned} \tag{1}$$

(note that if i, j are not consecutive, there is a small chance that $c_{1,i} = c_{1,j}$). Thus the c returned to the adversary has the property "c is the concatenation of identical blocks ($c_i = c_j$ for all i, j)" iff $c = \mathrm{Enc}_k(m_0)$. Therefore the adversary in the above experiment is actually correct 100% of the time, and breaks the encryption scheme. If this adversary is A,

$$\Pr[\mathrm{PrivK}^{eav}_{A,\Pi}(n) = 1] = 1 > \frac{1}{2} + negl(n), \tag{2}$$

for any negligible function $negl$.

. . . .

Problem 3 *Pseudorandom Things*

Let F be a pseudorandom function that maps n-bit strings to n-bit strings and uses n-bit keys. $G(s) \equiv F_x(1)||F_s(F_s(1))$ is a pseudorandom generator.

I will prove this by showing how a distinguisher for G could be used to create a distinguisher for F. Say that D distinguishes G such that, for any negligible function $negl(n)$,

$$|\Pr[D(G(s)) = 1] - \Pr[D(r) = 1]| = p > negl(n), \tag{3}$$

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 $r \in \{0,1\}^{2n}$.

Now construct distinguisher D' for F. D' starts by querying its oracle $\mathcal{O}$ on some arbitrary string $x \in \{0,1\}^n$, and saving $y_1 = \mathcal{O}(x)$. D' then saves $y_2 = \mathcal{O}(y_1)$ and $z = y_1 \mid\mid y_2$. D' then returns $D(z) = D(\mathcal{O}(x) \mid\mid \mathcal{O}(\mathcal{O}(x)))$.

When the oracle is F, D will return p, on average, because D' literally constructs outputs of G and sends those to D, which is a G-distinguisher. Further, by choosing x uniformly, D' ensures that the G-outputs sent to D are over a uniform sample of G's domain. When the oracle is $f \in \mathrm{Func}_n$ rather than F, z is just a uniform random string,and so $D(z)$ will return 0. Therefore, if a distinguisher D exists for G, then for the above construct a distinguisher D',

$$\left| \Pr[D^{F_k(\dot{})}(1^n) = 1] - \Pr[D^{f(\dot{})}(1^n) = 1] \right| = |p - 0| = p > negl(n), \tag{4}$$

for any negligible function $negl$. Yet because F is a pseudorandom function, we know that no such distinguisher could exist. Therefore no distinguisher for G could exist, and it is a pseudorandom generator (with expansion factor 2).

....

Problem 4 Security Table

	a	**b**	**c**	**d**
A	Y	Y	Y	Y
B	N	Y	N	N
C	N	Y	Y	Y
D	N	Y	Y	Y
E	N	N	N	N

....