George Mason University
CS 487/587: Cryptography

Prof. Foteini Baldimtsi
Homework 2: EAV Security and PRGs

Homework 2: EAV Security and PRGs

Submission policy. Submit your answers on Blackboard by 11:79pm Friday, **Sept. 17**, 2021. Your submission should include a .PDF file with all the answers to the theoretical problems. You should try to typeset your homeworks. Latex is especially recommended. No late submissions will be accepted. Your writeup MUST include the following information:

1. Your name and whether you take the class at **487** or **587** level.
2. List of references used (online material, course nodes, textbooks, wikipedia, etc.)

The homework will be graded by the class TA Anuj Pokhrel (apokhre@gmu.edu).

Exercise 1. ONLY IF in 587 level [20 points]
Solve part (a) of Exercise 2.13 from textbook.

Exercise 2. Substitution Cipher and EAV-Security [20 points]
Recall the Vigenere (or else poly-alphabetic substitution) cipher we discussed in Lecture 1 (and described in textbook pg. 13).
For simplicity consider the case where: $|K| = 2$ and $|M| = 4$ (i.e the size of the keys is 2 characters and the size of the message is 4 characters).

Show that the Vigenere cipher is not EAV-secure (as defined in class or per Definition 3.8 of textbook where $|m_0| = |m_1|$). As discussed in class, in order to show this you need to show a counterexample: i.e. describe an adversary who breaks the indistinguishability experiment with probability greater than $1/2 + \text{negl}(n)$, where n is the security parameter.

Exercise 3. PRGs [40 points] Let $G : \{0,1\}^n \rightarrow \{0,1\}^{2n}$ be a PRG (for every n), and let $s \in \{0,1\}^n$.

All the following constructions *are not* secure PRGs. For each one of them first state the expansion factor and then provide a counterexample to show that they are not PRGs, i.e. design a successful distinguisher and compute its advantage.

1. $G_a(s) = G(s)||G(s)$, where $||$ denotes concatenation.
2. $G_b(s) = G(s)||G(0^n)$, where 0^n denotes the all 0 string of length n.

3. $G_c(s) = G(1^{|s|}||s)$, where $1^{|s|}$ denotes the all 1 string of length equal to the length of s. (For this particular example you can assume that $G : \{0,1\}^{2n} \to \{0,1\}^{3n}$)

4. $G_d(s)$: first run $G(s) = x||y$ (where $|x| = |y| = n-$bits). Then run $G(y) = u||v$. Output $x||(y \oplus u)||v$. (Hint: in this particular example you can use Fact 2 for $H : \{0,1\}^n \to \{0,1\}^{3n}$).

Known Facts. Assume that the following facts hold (we might prove them secure later in class).

(1) if $H : \{0,1\}^n \to \{0,1\}^{4n}$ is a PRG, then $G(s) = H(s_1, \dots, s_{n/2})$ is also a PRG (where $s_1, \dots, s_{n/2}$ are the first $n/2$ bits of S).
(2) if $H : \{0,1\}^n \to \{0,1\}^{2n}$ is a PRG, then $G(s_L||s_R) = s_L||H(s_R)$ is also a PRG (where $s = s_L||s_R$ and $|s_L| = |s_R|$ (you can assume n is always even).

When working on any of the counterexamples above (a) - (d), the scheme should be insecure for *any* choice of $G()$, thus you can assume that $G()$ was constructed as above if needed.

Exercise 4. A bad reduction [40 points] Consider the following encryption scheme Π:

Let $G() : \{0,1\}^n \to \{0,1\}^{2n}$ be a secure PRG.

$\mathsf{Gen}(1^n)$: Output a key k of size n bits selected uniformly at random from $\{0,1\}^n$
$\mathsf{Enc}(k,m) : c = m_L \oplus G(k)||m_R \oplus G(k)$, (where $|m| = 4n$ bits and $|m_L| = |m_R| = 2n$ bits, and $||$ denotes string concatenation)
$\mathsf{Dec}(k,c) : m = c_L \oplus G(k)||c_R \oplus G(k)$

This scheme *is not* EAV secure. Your task is to find the mistake in the following reduction that attempts to prove EAV security of Π assuming that $G()$ is a secure PRG.

Break down your answer as follows:

1. (20 points) First prove that the scheme is not EAV secure (i.e. show how an adversary break the EAV game and with what probability it wins).

2. (20 points) Point out the flaw in the reduction and explain why it is wrong.

Bad Proof. We want to prove that if $G()$ is a secure PRG, then Π is a secure encryption scheme under the EAV security definition. We will do a proof by contradiction so we first state the contrapositive statement:

If Π is *not* a secure EAV encryption scheme, $G()$ is *not* a secure PRG.

To prove the contrapositive, we begin by assuming that Π is *not* a secure EAV encryption scheme, thus, there exists an adversary $\mathcal{A}$ that breaks the EAV security of Π with non-negligible advantage, i.e.

$$\Pr[\mathcal{A} \text{ breaks EAV of } \Pi] = \frac{1}{2} + p(n),$$

where $p(n)$ is a non-negligible value.
Then, using $\mathcal{A}$ we construct an distinguisher D that breaks the security of $G()$.

1. D is given as input a string w of size $2n$ from its challenger.
2. D starts running $\mathcal{A}$.
3. When $\mathcal{A}$ sends m_0, m_1 to D, D will first flip a bit $b \in \{0,1\}$, encrypt m_b as follows: $c^* = m_{b,L} \oplus w || m_{b,R} \oplus w$ and send c^* to $\mathcal{A}$.
4. $\mathcal{A}$ outputs a bit b'.
5. If $b' = b$ then D outputs 1 (i.e. claims that w was the output of a PRG), else D outputs 0.

Analysis. We consider 2 cases:

- Suppose w was a truly random string, then

$$\Pr[\mathcal{A} \text{ breaks EAV of } \Pi] = \frac{1}{2}$$

and thus $\Pr[D(r) = 1] = \frac{1}{2}$.
- Suppose w was the output of a PRG, then (by assumption)

$$\Pr[\mathcal{A} \text{ breaks EAV of } \Pi] = \frac{1}{2} + p(n),$$

and thus $\Pr[D(G(s)) = 1] = \frac{1}{2} + p(n)$.

Thus,

$$|\Pr[D(G(s)) = 1] - \Pr[D(r) = 1]| = |\frac{1}{2} + p(n) - \frac{1}{2}| = p(n)$$

and since $p(n)$ is a non-negligible value, D is a good distinguisher for $G()$, i.e. broke the security of the PRG $G()$.