Cryptography
CS 555

Topic 5: Constructing Secure Encryption Schemes

Homework 1 Released

- Due in class on Friday, February 3rd (2 weeks)
- Solutions should be typeset (preferably in Latex)
- You may collaborate with classmates, but you must write up your own solution and you *must understand* this solution
- One question covers PRFs which we will cover early next week.
- Clarification questions: spring-2017-cs-55500-wng@lists.purdue.edu

Recap

- Sematic Security/Indistinguishable Encryptions
- Concrete vs Asymptotic Security
  - Negligible Functions
  - Probabilistic Polynomial Time Algorithm

Today’s Goal

- ~~Define computational security~~

~~If you don’t understand what you want to achieve, how can you possibly know when (or if) you have achieved it?~~

- Show how to build a symmetric encryption scheme with semantic security.

- ~~Define computational security against an attacker who sees multiple ciphertexts or attempts to modify the ciphertexts~~

Building Blocks

- Pseudorandom Generators
- Stream Ciphers

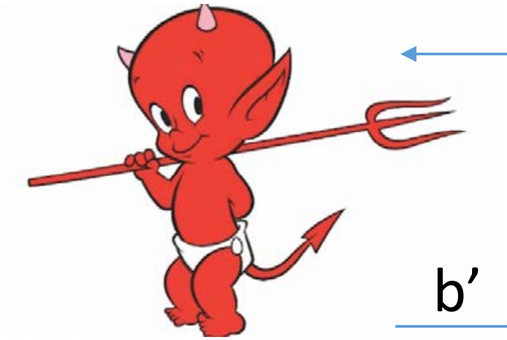
Pseudorandom Generator G

- **Input:** *Short* random seed $s \in \{0,1\}^n$
- **Output:** Longer "pseudorandom" string $G(s) \in \{0,1\}^{\ell(n)}$ with $\ell(n) > n$
  - $\ell(n)$ is called expansion factor

- **PRG Security**: For all PPT attacker A there is a negligible function negl s.t

$$\left|\Pr_{s\in\{0,1\}^n}\left[A\big(G(s)\big) = 1\right] - \Pr_{R\in\{0,1\}^{\ell(n)}}[A(R) = 1]\right| \le \mathrm{negl}(n)$$

PRG Security as a Game



R

b’

Random bit b

If b=1

$r \leftarrow \{0,1\}^n$

R = G(r)

Else

$0,1\}^{\ell(n)}$

ppt attacker

negligible function

$\forall$  $\Pr\Big[$  $Guesses\ b' = b\Big] \leq \frac{1}{2} + \mu(n)$

A Bad PRG

$$G(s) = s|1.$$

- What is the expansion factor?
  - Answer: $\ell(n)$=n+1

- Task: Construct a distinguisher D which breaks PRG security for G

  - One Answer: D(x|1)=1 and D(x|0)=0 for all x.
  - Analysis: Pr[D(G(s)) = 1] = ?
  - Analysis: Pr[D(R) = 1] = ?
  - $\left|\Pr_{s\in\{0,1\}^n}\left[D\left(G(s)\right) = 1\right] - \Pr_{R\in\{0,1\}^{\ell(n)}}[D(R) = 1]\right| = \frac{1}{2}$

One-Time-Pads + PRGs

- Encryption:
  - Secret key is the seed (K=s)

$$\mathrm{Enc}_s(\mathrm{m}) = \mathrm{G}(\mathrm{s}) \oplus m$$
$$\mathrm{Dec}_s(\mathrm{c}) = \mathrm{G}(\mathrm{s}) \oplus c$$

  - **Advantage**: $|\mathrm{m}| = \ell(n) \gg |s| = n$
  - Computational Security vs Information Theoretic (Perfect) Security
  - **Disadvantage**: Still can only send one message

Theorem 3.18: If G is a pseudorandom generator then the above encryption scheme has indistinguishable encryptions in the presence of an eavesdropper.

One-Time-Pads + PRGs

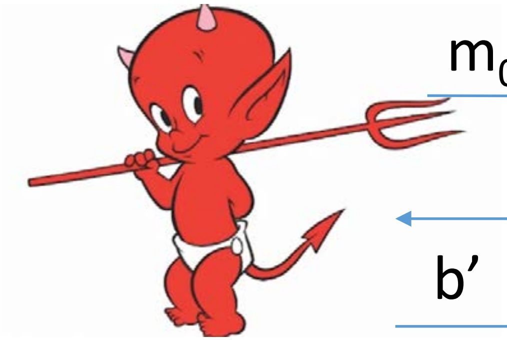
$$\mathrm{Enc}_s(\mathrm{m}) = \mathrm{G}(\mathrm{s}) \oplus m$$
$$\mathrm{Dec}_s(\mathrm{c}) = \mathrm{G}(\mathrm{s}) \oplus c$$

Theorem 3.18: If G is a pseudorandom generator then the above encryption scheme has indistinguishable encryptions in the presence of an eavesdropper.

Proof by Reduction: Start with and attacker A that breaks security of encryption scheme and transform A into distinguisher D that breaks PRG security of G.

Why is this sufficient?

Breaking Semantic Security



m_0, m_1

$c = G(s) \oplus m_b$

b'

Random bit b
Random seed s

$ppt\ attacker$

$non-negligible\ function$
(possibly still small)

$\Pr\Big[$  $Guesses\ b' = b\Big] \geq \frac{1}{2} + f(n)$

The Reduction

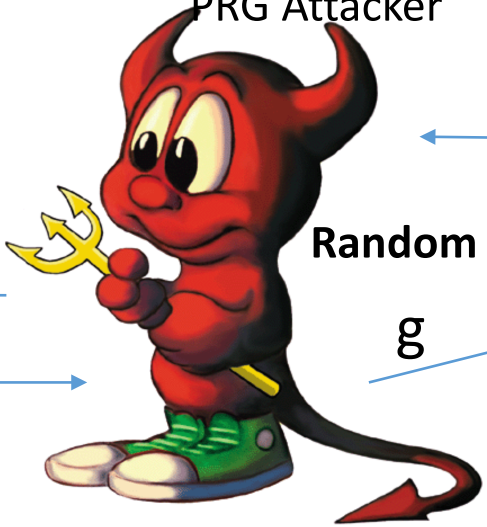
Encryption Attacker

m_0, m_1

$c = R \oplus m_{b'}$

b''

PRG Attacker



R

Random b'

g

Random bit b

If b=1

$r \leftarrow \{0,1\}^n$

$R = G(r)$

Else

$R \leftarrow \{0,1\}^{\ell(n)}$

- What is $\Pr[b'' \neq b' | b=0]$?
  - Hint: What encryption scheme is used?
- What is $\Pr[b'' = b' | b=1]$?

$$g = \begin{cases} 1 & \text{if } b=b' \\ 0 & \text{otherwise} \end{cases}$$

Analysis

$$\left|\Pr_{s\in\{0,1\}^n}\left[D\left(G(s)\right) = 1\right] - \Pr_{R\in\{0,1\}^{\ell(n)}}\left[D(R) = 1\right]\right|$$

$$= |\Pr[b'' = b'|b=1] - \Pr[b'' \neq b'|b=0]|$$

$$= |\Pr[b'' = b'|b=1] - ½|$$

$$\geq ½ + f(n) - ½ \geq f(n)$$

Recall: f(n) was (non-negligible) advantage of encryption attacker.

Implication: PRG G is also insecure (contrary to assumption).

QED

Candidate PRG

- **Notation:** Given string $x \in \{0,1\}^n$ and a subset $S \subset \{1, \dots, n\}$ let $x_S \in \{0,1\}^{|S|}$ denote the substring formed by concatenating bits at the positions in S.
- **Example**: x=10110 and S = {1,4,5} x_S=110

$$P(x_1, x_2, x_3, x_4, x_5) = x_1 + x_2 + x_3 + x_4 x_5 \bmod 2$$

- Select random subsets $\mathbb{S} = S_1, \dots, S_{\ell(n)} \subset \{1, \dots, n\}$ of size $|S_i|$=5 and with $\ell(n) = n^{1.4}$

$$G_{\mathbb{S}}(x) = P\left(x_{S_1}\right) | \dots \left| P\left(x_{S_{\ell(n)}}\right)\right.$$

Stream Cipher vs PRG

- PRG pseudorandom bits output all at once
- Stream Cipher
  - Pseudorandom bits can be output as a stream
  - RC4, RC5 (Ron's Code)

st_0 := Init(s)

For i=1 to ℓ:

    (y_i, st_i):=GetBits(st_{i-1})

Output: $y_1, \ldots, y_\ell$

The RC4 Stream Cipher

- A proprietary cipher owned by RSA, designed by Ron Rivest in 1987.
- Became public in 1994.
- Simple and effective design.
- Variable key size (typical 40 to 256 bits),
- Output unbounded number of bytes.
- Widely used (web SSL/TLS, wireless WEP).
- Extensively studied, not a completely secure PRNG, when used correctly, ~~no known attacks exist~~
- **Newer Versions**: RC5 and RC6
- **Rijndael** selected by NIST as AES in 2000

The RC4 Cipher

- The cipher internal state consists of
  - a 256-byte array S, which contains a permutation of 0 to 255
    - total number of possible states is $256! \approx 2^{1700}$
  - two indexes: i, j

```
i = j = 0
Loop
   i = (i + 1) (mod 256)
   j = (j + S[i]) (mod 256)
   swap(S[i], S[j])
   output (S[i] + S[j]) (mod 256)
End Loop
```

Limitations of Current Security Definition

- Assumes adversary observes just one ciphertext

- What if adversary observes two ciphertexts?

$$c_1 = \mathrm{Enc}_{\mathrm{s}}(m_1) = \mathrm{G}(s) \oplus m_1$$
$$c_2 = \mathrm{Enc}_{\mathrm{s}}(m_2) = \mathrm{G}(s) \oplus m_2$$

- How could the adversary (Joe) attempt to modify c=Enc_k(m) below?

m = “Pay Joe the following amount (USD): 000000101”

Coming Up…

- Before Next Class (Friday)
  - Read: Katz and Lindell 3.4
  - Security for Multiple Encryptions