Lecture 4 – Pseudorandom Functions

CS466 - Applied Cryptography

Adam O’Neill

adapted from http://cseweb.ucsd.edu/~mihir/cse107/

What is a "good" blockcipher?

We want to define a notion of a "good" blockcipher, where "good" means natural uses of the blockcipher are secure.

One idea is to list requirements:

- Key recovery is hard.
- Message recovery is hard.

Analogy to Intelligence

What if we want to define the notion of "intelligent" for a computer program?

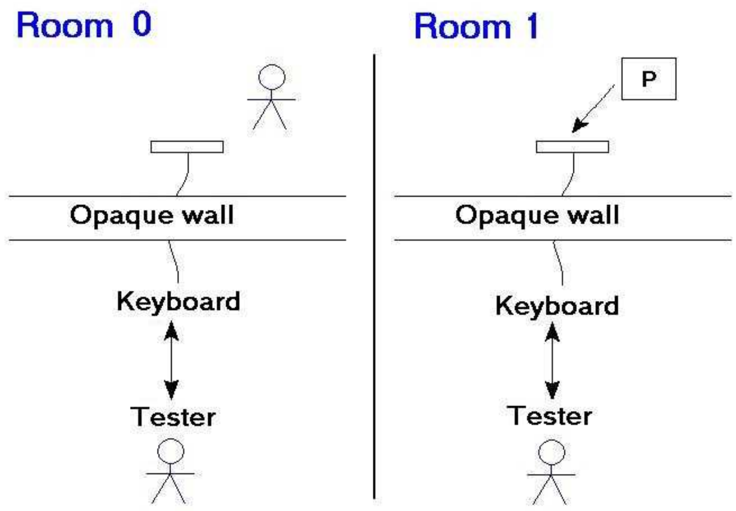
Again, one idea is to list requirements:

- It can be happy.
- It can multiply numbers
- … but only small numbers.

Turing’s Answer

A program is “intelligent” if its input/output behavior is indistinguishable from that of a human.

The Turing Test



Game:

- Put tester in room 0 and let it interact with object behind wall
- Put tester in rooom 1 and let it interact with object behind wall
- Now ask tester: which room was which?

The measure of "intelligence" of P is the extent to which the tester fails.

The Analogy

Notion	Real object	Ideal object
Intelligence	Program	Human
PRF	Block cipher	?

good blockcipher

"wants to be like"

RANDOM FUNCTION

Playing with Probabilities

Suppose $f:\{0,1\}^l \to \{0,1\}^l$ is randomly chosen from $\underbrace{Func(\{0,1\}^l, \{0,1\}^l)}$

set of all functions from $\{0,1\}^l \to \{0,1\}^l$

$$\Pr_f[f(0^l) = 0^l] = 2^{-l}$$

$$\Pr_f[f(0^l) = f(1^l)] = 2^{-l}$$

$$\Pr[f(0^l) \oplus f(1^l) = 0^l] = 2^{-l}$$

Function Families

A family of functions F : Keys(F) $\times$ Dom(F) $\rightarrow$ Range(F) is a two-argument map. For $K \in$ Keys(F) we let F_K : Dom(F) $\rightarrow$ Range(F) be defined by

$$\forall x \in \text{Dom}(F) : F_K(x) = F(K, x)$$

This generalizes the notion of a blockcipher

→ Keys(F) = $\{0,1\}^k$

Dom(F) = $\{0,1\}^l$ = Range(F)

$F_K(x)$ is a permutation for all K.

Both $F_K(\cdot)$ & $F_K^{-1}(\cdot)$ are efficiently computable

Intuition

Adversary interacts with either

(1) the real function (keyed by an unknown random $K \in Keys(F)$)

recall by Kerkoff's principle the adversary KNOWS the function $F: Keys(F) \times Dom(F) \to RANGE(F)$

(2) A TRULY RANDOM function from $\{0,1\}^{\ell} \to \{0,1\}^{\ell}$

adversary submits inputs and is given back the output. GUESSES which "world" its in

The Games

Let F: $\text{Keys}(F) \times \text{Dom}(F) \to \mathrm{Range}(F)$ be a family of functions.

Game Real_F	Game $\mathrm{Rand}_{\text{Range}(F)}$
procedure Initialize $K \xleftarrow{\$} \text{Keys}(F)$ **procedure Fn**(x) Return $F_K(x)$	**procedure Fn**(x) $\text{T}[x] \xleftarrow{\$} \text{Range}(F)$ Return $\text{T}[x]$

over coins of game & coins of adversary

Associated to F, A are the probabilities

$$\Pr\left[\mathrm{Real}_F^A \Rightarrow 1\right] \qquad \Big| \qquad \Pr\left[\mathrm{Rand}_{\text{Range}(F)}^A \Rightarrow 1\right]$$

that A outputs 1 in each world. The advantage of A is

measure of success →

$$\mathbf{Adv}_F^{\mathrm{prf}}(A) = \Pr\left[\mathrm{Real}_F^A \Rightarrow 1\right] - \Pr\left[\mathrm{Rand}_{\text{Range}(F)}^A \Rightarrow 1\right]$$

Advantage Interpretation

$$\mathbf{Adv}_F^{\mathrm{prf}}(A) = \Pr\left[\mathrm{Real}_F^A \Rightarrow 1\right] - \Pr\left[\mathrm{Rand}_{\mathsf{Range}(F)}^A \Rightarrow 1\right]$$

A “large” (close to 1) advantage means

- A is doing well
- F is not secure

A “small” (close to 0 or ≤ 0) advantage means

- A is doing poorly
- F resists the attack A is mounting

$2^k \cdot T_E \cdot q + q\log q$

time to compute E — to make queries

PRF Security

$$\mathbf{Adv}_F^{\mathrm{prf}}(A) = \Pr\left[\mathrm{Real}_F^A \Rightarrow 1\right] - \Pr\left[\mathrm{Rand}_{\mathsf{Range}(F)}^A \Rightarrow 1\right]$$

Security: F is a (secure) PRF if $\mathbf{Adv}_F^{\mathrm{prf}}(A)$ is "small" for ALL A that use "practical" amounts of resources.

Insecurity: F is insecure (not a PRF) if there exists A using "few" resources that achieves "high" advantage.

Examples

One-time pad blockcipher

$E : \{0,1\}^k \times \{0,1\}^k \to \{0,1\}^k$ where

$E_K(x) \stackrel{def}{=} x \oplus K$.

Let's ~~~~ show this is not a PRF:

Adversary A

$y \leftarrow Fn(0^\ell)$

$x' \leftarrow Fn(y)$

If $x' = 0^\ell$ Ret 1

Else return 0

Claim 1: $\Pr[\mathrm{REAL}_E^A \Rightarrow 1] = 1$.

Claim 2: $\Pr[\mathrm{RAND}_{\{0,1\}^k}^A \Rightarrow 1] = 2^{-\ell}$

proof of claim 1:

By def of E we have

$$Fn(0^\ell) = 0^k \oplus K = K$$

$$= Fn(K) = K \oplus K = 0^\ell \checkmark$$

proof of claim 2:

Consider an execution of $\mathrm{RAND}_{\{0,1\}^k}^A$ after $Fn(0^\ell)$ is fixed, i.e. y is fixed. Then $Fn(y)$ is independently random so

$$\Pr[Fn(y) = 0^k] = 2^{-k}. \checkmark$$

Birthday Attack

Pick $y_1, \ldots, y_q \stackrel{\$}{\leftarrow} \{1, \ldots, N\}$ and let

Let

$$C(N, q) = \Pr\left[y_1, \ldots, y_q \textbf{ not } \text{all distinct}\right]$$

Fact: Then

$$0.3 \cdot \frac{q(q-1)}{N} \leq C(N, q) \leq 0.5 \cdot \frac{q(q-1)}{N}$$

where the lower bound holds for $1 \leq q \leq \sqrt{2N}$.

Analysis

Conclusion: If $E : \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}^\ell$ is a block cipher, there is an attack on it as a PRF that succeeds in about $2^{\ell/2}$ queries.

Depends on block length, not key length!

	ℓ	$2^{\ell/2}$	Status
DES, 2DES, 3DES3	64	2^{32}	Insecure
AES	128	2^{64}	Secure

PRF-Security Implications

PRF-security can be seen as a "master property" for blockciphers that implies all other security properties we want.

E.g., we can show that PRF-security implies security against key-recovery.

Reduction Sketch

Conclusion

- We believe DES, AES are “good” blockciphers in the sense that there is no significantly “better than generic” attacks under the PRF notion.
- Generic attacks:
  - Exhaustive key-search.
  - Birthday attack.