PSEUDO-RANDOM FUNCTIONS
Recall

We studied security of a block cipher against key recovery.

But we saw that security against key recovery is not sufficient to ensure that natural usages of a block cipher are secure.

We want to answer the question:

What is a good block cipher?

where “good” means that natural uses of the block cipher are secure.

We could try to define “good” by a list of necessary conditions:

- Key recovery is hard
- Recovery of $M$ from $C = E_K(M)$ is hard
- ... 

But this is neither necessarily correct nor appealing.
Q: What does it mean for a program to be “intelligent” in the sense of a human?

Possible answers:
- It can be happy
- It recognizes pictures
- It can multiply
- But only small numbers!
- 
- 
- Clearly, no such list is a satisfactory answer to the question.
Q: What does it mean for a program to be “intelligent” in the sense of a human?

Turing’s answer: A program is intelligent if its input/output behavior is indistinguishable from that of a human.
Turing Intelligence Test

Behind the wall:

- Room 1: The program $P$
- Room 0: A human
Turing Intelligence Test

Game:

• Put tester in room 0 and let it interact with object behind wall
• Put tester in room 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.
<table>
<thead>
<tr>
<th>Notion</th>
<th>Real object</th>
<th>Ideal object</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intelligence</td>
<td>Program</td>
<td>Human</td>
</tr>
<tr>
<td>PRF</td>
<td>Block cipher</td>
<td>?</td>
</tr>
<tr>
<td>Notion</td>
<td>Real object</td>
<td>Ideal object</td>
</tr>
<tr>
<td>------------</td>
<td>----------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>Intelligence</td>
<td>Program</td>
<td>Human</td>
</tr>
<tr>
<td>PRF</td>
<td>Block cipher</td>
<td>Random function</td>
</tr>
</tbody>
</table>
Random functions

Game $\text{Rand}_R$  // here $R$ is a set

procedure $\text{Fn}(x)$
if $T[x] = ⊥$ then $T[x] \leftarrow^S R$
return $T[x]$

Adversary $A$
- Make queries to $\text{Fn}$
- Eventually halts with some output

We denote by
$$\Pr \left[ \text{Rand}_R^A \Rightarrow d \right]$$
the probability that $A$ outputs $d$
Random functions

Game $\text{Rand}_{\{0,1\}^3}$

procedure $\text{Fn}(x)$
if $T[x] = \bot$ then $T[x] \leftarrow \{0, 1\}^3$
return $T[x]$

adversary $A$

$y \leftarrow \text{Fn}(01)$
return $(y = 000)$

$\Pr \left[ \text{Rand}_A^{\{0,1\}^3} \Rightarrow \text{true} \right] = \frac{9}{44}$
Game $\text{Rand}_{\{0,1\}^3}$

procedure $\text{Fn}(x)$

if $T[x] = \bot$ then $T[x] \leftarrow \{0, 1\}^3$

return $T[x]$

adversary $A$

$y \leftarrow \text{Fn}(01)$

return $(y = 000)$

$$\Pr \left[ \text{Rand}^A_{\{0,1\}^3} \Rightarrow \text{true} \right] = 2^{-3}$$
Random function

Game $\text{Rand}_{\{0,1\}^3}$

**procedure** $\text{Fn}(x)$

if $T[x] = \bot$ then $T[x] \leftarrow \{0, 1\}^3$

return $T[x]$

**adversary** $A$

$y_1 \leftarrow \text{Fn}(00)$

$y_2 \leftarrow \text{Fn}(11)$

return $(y_1 = 010 \land y_2 = 011)$

$$
\Pr \left[ \text{Rand}^A_{\{0,1\}^3} \Rightarrow \text{true} \right] =
$$
Random function

Game $\text{Rand}_{\{0,1\}^3}$

**procedure $\text{Fn}(x)$**
if $T[x] = \bot$ then $T[x] \leftarrow \{0, 1\}^3$
return $T[x]$

adversary $A$
$y_1 \leftarrow \text{Fn}(00)$
$y_2 \leftarrow \text{Fn}(11)$
return $(y_1 = 010 \land y_2 = 011)$

$$\Pr \left[ \text{Rand}_{\{0,1\}^3} \Rightarrow \text{true} \right] = 2^{-6}$$
Game \( \text{Rand}_{\{0,1\}^3} \)

**procedure** \( \text{Fn}(x) \)

if \( T[x] = \perp \) then \( T[x] \leftarrow \{0, 1\}^3 \)

return \( T[x] \)

**adversary** \( A \)

\( y_1 \leftarrow \text{Fn}(00) \)

\( y_2 \leftarrow \text{Fn}(11) \)

return \((y_1 \oplus y_2 = 101)\)

\[
\Pr \left[ \text{Rand}_A^{\{0,1\}^3} \Rightarrow \text{true} \right] = \quad
\]
Random function

Game $\text{Rand}_{\{0,1\}^3}$

**procedure** $\text{Fn}(x)$

if $T[x] = \bot$ then $T[x] \leftarrow \{0, 1\}^3$

return $T[x]$

**adversary** $A$

$y_1 \leftarrow \text{Fn}(00)$

$y_2 \leftarrow \text{Fn}(11)$

return $(y_1 \oplus y_2 = 101)$

$$\Pr \left[ \text{Rand}_A^{\{0,1\}^3} \Rightarrow \text{true} \right] = 2^{-3}$$
A family of functions $F : \text{Keys}(F) \times \text{Dom}(F) \rightarrow \text{Range}(F)$ is a two-argument map. For $K \in \text{Keys}(F)$ we let $F_K : \text{Dom}(F) \rightarrow \text{Range}(F)$ be defined by

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

Examples:

- **DES**: $\text{Keys}(F) = \{0, 1\}^{56}$, $\text{Dom}(F) = \text{Range}(F) = \{0, 1\}^{64}$
- **Any block cipher**: $\text{Dom}(F) = \text{Range}(F)$ and each $F_K$ is a permutation
### Real versus Ideal

<table>
<thead>
<tr>
<th>Notion</th>
<th>Real object</th>
<th>Ideal object</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRF</td>
<td>Family of functions (eg. a block cipher)</td>
<td>Random function</td>
</tr>
</tbody>
</table>

$F$ is a PRF if the input-output behavior of $F_K$ looks to a tester like the input-output behavior of a random function.

Tester does **not** get the key $K$!
Games defining prf advantage of an adversary against $F$

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

Associated to $F$, $A$ are the probabilities

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

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

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

<table>
<thead>
<tr>
<th>A’s output $d$</th>
<th>Intended meaning: I think I am in game</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Real</td>
</tr>
<tr>
<td>0</td>
<td>Random</td>
</tr>
</tbody>
</table>

$\text{Adv}_F^{\text{prf}} (A) \approx 1$ means $A$ is doing well and $F$ is not prf-secure.

$\text{Adv}_F^{\text{prf}} (A) \approx 0$ (or $\leq 0$) means $A$ is doing poorly and $F$ resists the attack $A$ is mounting.
Adversary advantage depends on its
- strategy
- resources: Running time $t$ and number $q$ of oracle queries

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

**Example**: 80-bit security could mean that for all $n = 1, \ldots, 80$ we have

$$\text{Adv}^\text{prf}_F(A) \leq 2^{-n}$$

for any $A$ with time and number of oracle queries at most $2^{80-n}$.

**Insecurity**: $F$ is insecure (not a PRF) if we can specify an $A$ using “few” resources that achieves “high” advantage.
Define $F : \{0, 1\}^\ell \times \{0, 1\}^\ell \to \{0, 1\}^\ell$ by $F_K(x) = K \oplus x$ for all $K, x \in \{0, 1\}^\ell$. Is $F$ a secure PRF?

So we are asking: Can we design a low-resource $A$ so that

$$\text{Adv}_{F}^{\text{prf}}(A) = \Pr \left[ \text{Real}_F^{A} \Rightarrow 1 \right] - \Pr \left[ \text{Rand}_{\{0,1\}^\ell}^{A} \Rightarrow 1 \right]$$

is close to 1?
Example

Define $F : \{0, 1\}^\ell \times \{0, 1\}^\ell \to \{0, 1\}^\ell$ by $F_K(x) = K \oplus x$ for all $K, x \in \{0, 1\}^\ell$. Is $F$ a secure PRF?

Game $\text{Real}_F$

procedure Initialize
$K \leftarrow \text{Keys}(F)$

procedure $F_n(x)$
Return $K \oplus x$

Game $\text{Rand}_{\{0,1\}^\ell}$

procedure $F_n(x)$
if $T[x] = \perp$ then $T[x] \leftarrow \{0, 1\}^\ell$
Return $T[x]$

So we are asking: Can we design a low-resource $A$ so that

$$\text{Adv}_{\text{prf}}^F(A) = \Pr \left[ \text{Real}_F^A \Rightarrow 1 \right] - \Pr \left[ \text{Rand}_{\{0,1\}^\ell}^A \Rightarrow 1 \right]$$

is close to 1?

Exploitable weakness of $F$: For all $K$ we have

$$F_K(0^\ell) \oplus F_K(1^\ell) = (K \oplus 0^\ell) \oplus (K \oplus 1^\ell) = 1^\ell$$
Example: The adversary

\[ F: \{0, 1\}^\ell \times \{0, 1\}^\ell \rightarrow \{0, 1\}^\ell \] is defined by \( F_K(x) = K \oplus x \).

adversary \( A \)
if \( F_n(0^\ell) \oplus F_n(1^\ell) = 1^\ell \) then return 1 else return 0
Example: Real game analysis

\[
F: \{0, 1\}^\ell \times \{0, 1\}^\ell \rightarrow \{0, 1\}^\ell \text{ is defined by } F_K(x) = K \oplus x.
\]

adversary \( A \)
if \( F_n(0^\ell) \oplus F_n(1^\ell) = 1^\ell \) then return 1 else return 0

Game \( \text{Real}_F \)

procedure Initialize
\( K \leftarrow \text{Keys}(F) \)

procedure \( F_n(x) \)
Return \( K \oplus x \)

\[
\Pr \left[ \text{Real}_F^A \Rightarrow 1 \right] = \]
Example: Real game analysis

\[ F: \{0, 1\}^\ell \times \{0, 1\}^\ell \rightarrow \{0, 1\}^\ell \text{ is defined by } F_K(x) = K \oplus x. \]

**adversary** \( A \)

if \( F_n(0^\ell) \oplus F_n(1^\ell) = 1^\ell \) then return 1 else return 0

---

**Game Real\(_F\)**

**procedure Initialize**

\[ K \leftarrow \text{Keys}(F) \]

**procedure \( F_n(x) \)**

Return \( K \oplus x \)

\[
\Pr\left[ \text{Real}_F^A \Rightarrow 1 \right] = 1
\]

because

\[
F_n(0^\ell) \oplus F_n(1^\ell) = F_K(0^\ell) \oplus F_K(1^\ell) = (K \oplus 0^\ell) \oplus (K \oplus 1^\ell) = 1^\ell
\]
Example: Rand game analysis

\[ F: \{0, 1\}^\ell \times \{0, 1\}^\ell \rightarrow \{0, 1\}^\ell \text{ is defined by } F_K(x) = K \oplus x. \]

adversary \( A \)

if \( F_n(0^\ell) \oplus F_n(1^\ell) = 1^\ell \) then return 1 else return 0

\[
\text{Game } \text{Rand}_{\{0,1\}^\ell}
\]

**procedure** \( F_n(x) \)

if \( T[x] = \perp \) then \( T[x] \leftarrow^\$ \{0, 1\}^\ell \)

Return \( T[x] \)

\[
\Pr \left[ \text{Rand}_{\{0,1\}^\ell}^A \Rightarrow 1 \right] =
\]
Example: Rand game analysis

\[ F: \{0, 1\}^\ell \times \{0, 1\}^\ell \to \{0, 1\}^\ell \] is defined by \( F_K(x) = K \oplus x \).

Adversary \( A \)

if \( F_n(0^\ell) \oplus F_n(1^\ell) = 1^\ell \) then return 1 else return 0

\[
\text{Game Rand}_{\{0,1\}^\ell}^A
\]

\textbf{procedure} \( F_n(x) \)

if \( T[x] = \bot \) then \( T[x] \leftarrow \{0, 1\}^\ell \)
Return \( T[x] \)

\[
\Pr \left[ \text{Rand}_{\{0,1\}^\ell}^A \Rightarrow 1 \right] = \Pr \left[ F_n(1^\ell) \oplus F_n(0^\ell) = 1^\ell \right] =
\]
Example: Rand game analysis

\[ F : \{0, 1\}^\ell \times \{0, 1\}^\ell \rightarrow \{0, 1\}^\ell \text{ is defined by } F_K(x) = K \oplus x. \]

adversary \( A \)
if \( F_n(0^\ell) \oplus F_n(1^\ell) = 1^\ell \) then return 1 else return 0

\[
\text{Game } \text{Rand}_{\{0,1\}}^\ell \\
\text{procedure } F_n(x) \\
\text{if } T[x] = \bot \text{ then } T[x] \leftarrow \{0, 1\}^\ell \\
\text{Return } T[x]
\]

\[
\Pr \left[ \text{Rand}_A^{\{0,1\}^\ell} \Rightarrow 1 \right] = \Pr \left[ F_n(1^\ell) \oplus F_n(0^\ell) = 1^\ell \right] = 2^{-\ell}
\]

because \( F_n(0^\ell), F_n(1^\ell) \) are random \( \ell \)-bit strings.
Example: Conclusion

\[ F: \{0, 1\}^\ell \times \{0, 1\}^\ell \rightarrow \{0, 1\}^\ell \] is defined by \( F_K(x) = K \oplus x \).

adversary \( A \)

if \( F_n(0^\ell) \oplus F_n(1^\ell) = 1^\ell \) then return 1 else return 0

Then

\[
\text{Adv}_F^{\text{prf}}(A) = \frac{1}{2} \cdot \text{Pr}[\text{Real}_F^A \Rightarrow 1] - \text{Pr}[\text{Rand}_A^{\{0,1\}^\ell} \Rightarrow 1] = 1 - 2^{-\ell}
\]

and \( A \) is efficient.

Conclusion: \( F \) is not a secure PRF.
Define the family of functions $F: \{0, 1\}^{128} \times \{0, 1\}^{128} \rightarrow \{0, 1\}^{128}$ by $F(K, M) = AES(M, K)$. Assuming AES is a secure PRF, is $F$ a secure PRF? If so, explain why. If not, present the best attack (with analysis) that you can.

If you give an attack it should be presented in the format of the above examples, with an adversary clearly specified in pseudo-code, a claim about its advantage, and a succinct proof of the claim. Avoid long textual descriptions.
Birthday Problem

$q$ people $1, \ldots, q$ with birthdays

$$y_1, \ldots, y_q \in \{1, \ldots, 365\}$$

Assume each person’s birthday is a random day of the year. Let

$$C(365, q) = \Pr[2 \text{ or more persons have same birthday}]$$

$$= \Pr[y_1, \ldots, y_q \text{ are not all different}]$$

- What is the value of $C(365, q)$?
- How large does $q$ have to be before $C(365, q)$ is at least 1/2?
Birthday Problem

$q$ people $1, \ldots, q$ with birthdays

$$y_1, \ldots, y_q \in \{1 \ldots, 365\}$$

Assume each person’s birthday is a random day of the year. Let

$$C(365, q) = \Pr[2 \text{ or more persons have same birthday}]$$

$$= \Pr[y_1, \ldots, y_q \text{ are not all different}]$$

• What is the value of $C(365, q)$?
• How large does $q$ have to be before $C(365, q)$ is at least $1/2$?

Naive intuition:

• $C(365, q) \approx q/365$
• $q$ has to be around 365
Birthday Problem

$q$ people 1, \ldots, $q$ with birthdays

\[ y_1, \ldots, y_q \in \{1 \ldots, 365\} \]

Assume each person’s birthday is a random day of the year. Let

\[ C(365, q) = \Pr [\text{2 or more persons have same birthday}] = \Pr [y_1, \ldots, y_q \text{ are not all different}] \]

• What is the value of $C(365, q)$?
• How large does $q$ have to be before $C(365, q)$ is at least 1/2?

Naive intuition:
• $C(365, q) \approx q/365$
• $q$ has to be around 365

The reality
• $C(365, q) \approx q^2/365$
• $q$ has to be only around 23
Birthday collision bounds

$C(365, q)$ is the probability that some two people have the same birthday in a room of $q$ people with random birthdays

<table>
<thead>
<tr>
<th>$q$</th>
<th>$C(365, q)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>0.253</td>
</tr>
<tr>
<td>18</td>
<td>0.347</td>
</tr>
<tr>
<td>20</td>
<td>0.411</td>
</tr>
<tr>
<td>21</td>
<td>0.444</td>
</tr>
<tr>
<td>23</td>
<td>0.507</td>
</tr>
<tr>
<td>25</td>
<td>0.569</td>
</tr>
<tr>
<td>27</td>
<td>0.627</td>
</tr>
<tr>
<td>30</td>
<td>0.706</td>
</tr>
<tr>
<td>35</td>
<td>0.814</td>
</tr>
<tr>
<td>40</td>
<td>0.891</td>
</tr>
<tr>
<td>50</td>
<td>0.970</td>
</tr>
</tbody>
</table>
Pick $y_1, \ldots, y_q \leftarrow \{1, \ldots, N\}$ and let

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

Birthday setting: $N = 365$
Birthday Problem

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

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

Birthday setting: $N = 365$

Fact: $C(N, q) \approx \frac{q^2}{2N}$
Let $y_1, \ldots, y_q \leftarrow \{1, \ldots, N\}$. Then

$$1 - C(N, q) = \Pr[y_1, \ldots, y_q \text{ all distinct}]$$

$$= 1 \cdot \frac{N - 1}{N} \cdot \frac{N - 2}{N} \cdots \frac{N - (q - 1)}{N}$$

$$= \prod_{i=1}^{q-1} \left(1 - \frac{i}{N}\right)$$

so

$$C(N, q) = 1 - \prod_{i=1}^{q-1} \left(1 - \frac{i}{N}\right)$$
Birthday bounds

Let

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

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 \( 1 \leq q \leq \sqrt{2N} \).
Let \( E : \{0, 1\}^k \times \{0, 1\}^\ell \rightarrow \{0, 1\}^\ell \) be a block cipher.

Can we design \( A \) so that

\[
\text{Adv}_{E}^{\text{prf}}(A) = \Pr[\text{Real}_E \Rightarrow 1] - \Pr[\text{Rand}_{\{0,1\}^\ell} \Rightarrow 1]
\]

is close to 1?
Defining property of a block cipher: $E_K$ is a permutation for every $K$

So if $x_1, \ldots, x_q$ are distinct then

- $F_n = E_K \Rightarrow F_n(x_1), \ldots, F_n(x_q)$ distinct
- $F_n$ random $\Rightarrow F_n(x_1), \ldots, F_n(x_q)$ not necessarily distinct

This leads to the following attack:

**adversary** $A$

Let $x_1, \ldots, x_q \in \{0, 1\}^\ell$ be distinct

for $i = 1, \ldots, q$ do $y_i \leftarrow F_n(x_i)$

if $y_1, \ldots, y_q$ are all distinct then return 1
else return 0
Let $E : \{0, 1\}^k \times \{0, 1\}^\ell \to \{0, 1\}^\ell$ be a block cipher

<table>
<thead>
<tr>
<th>Procedure Initialize</th>
</tr>
</thead>
<tbody>
<tr>
<td>$K \leftarrow {0, 1}^k$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Procedure $\text{Fn}(x)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Return $E_K(x)$</td>
</tr>
</tbody>
</table>

**adversary $A$**

Let $x_1, \ldots, x_q \in \{0, 1\}^\ell$ be distinct

for $i = 1, \ldots, q$ do $y_i \leftarrow \text{Fn}(x_i)$

if $y_1, \ldots, y_q$ are all distinct

then return 1 else return 0

Then

$$\Pr \left[ \text{Real}_E^A \Rightarrow 1 \right] =$$
Let $E : \{0, 1\}^k \times \{0, 1\}^\ell \rightarrow \{0, 1\}^\ell$ be a block cipher

**Game Real$_E$**

**procedure Initialize**

$K \leftarrow \{0, 1\}^k$

**procedure Fn(x)**

Return $E_K(x)$

**adversary $A$**

Let $x_1, \ldots, x_q \in \{0, 1\}^\ell$ be distinct

for $i = 1, \ldots, q$ do $y_i \leftarrow \text{Fn}(x_i)$

if $y_1, \ldots, y_q$ are all distinct then return 1 else return 0

Then

$$\Pr \left[ \text{Real}_E^A \Rightarrow 1 \right] = 1$$

because $y_1, \ldots, y_q$ will be distinct because $E_K$ is a permutation.
Let $E : \{0, 1\}^K \times \{0, 1\}^\ell \rightarrow \{0, 1\}^\ell$ be a block cipher

**Game** Rand$_{\{0,1\}^\ell}$

**procedure** Fn($x$)

if $T[x] = \perp$ then $T[x] \leftarrow \{0, 1\}^\ell$

Return $T[x]$

**adversary** $A$

Let $x_1, \ldots, x_q \in \{0, 1\}^\ell$ be distinct for $i = 1, \ldots, q$ do $y_i \leftarrow$ Fn($x_i$) if $y_1, \ldots, y_q$ are all distinct then return 1 else return 0

Then

$$\Pr \left[ \text{Rand}_A^{\{0,1\}^\ell} \Rightarrow 1 \right] = \Pr [y_1, \ldots, y_q \text{ all distinct}] = 1 - C(2^\ell, q)$$

because $y_1, \ldots, y_q$ are randomly chosen from $\{0, 1\}^\ell$. 
Birthday attack on a block cipher

Let $x_1, \ldots, x_q \in \{0, 1\}^\ell$ be distinct
for $i = 1, \ldots, q$ do $y_i \leftarrow F_n(x_i)$
if $y_1, \ldots, y_q$ are all distinct then return 1 else return 0

$$\text{Adv}_{E}^{\text{prf}}(A) = \Pr \left[ \text{Real}_E^A \Rightarrow 1 \right] - \Pr \left[ \text{Rand}_\{0,1\}^\ell \Rightarrow 1 \right]$$

$$= C(2^\ell, q) \geq 0.3 \cdot \frac{q(q-1)}{2^\ell}$$

so

$q \approx 2^{\ell/2} \Rightarrow \text{Adv}_{E}^{\text{prf}}(A) \approx 1.$
Conclusion: If $E : \{0, 1\}^k \times \{0, 1\}^\ell \rightarrow \{0, 1\}^\ell$ 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!

<table>
<thead>
<tr>
<th></th>
<th>$\ell$</th>
<th>$2^{\ell/2}$</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>DES, 2DES, 3DES</td>
<td>64</td>
<td>$2^{32}$</td>
<td>Insecure</td>
</tr>
<tr>
<td>AES</td>
<td>128</td>
<td>$2^{64}$</td>
<td>Secure</td>
</tr>
</tbody>
</table>
We have seen two possible metrics of security for a block cipher $E$

- **KR-security**: It should be hard to find a key consistent with input-output examples of a hidden target key.
- **PRF-security**: It should be hard to distinguish the input-output behavior of $E_K$ from that of a random function.

**Fact**: PRF-security of $E$ implies

- KR-security of $E$
- Many other security attributes of $E$

This is a validation of the choice of PRF security as our main metric.
If $E$ is PRF-secure then it is KR-secure

**Proposition:** Let $E : \{0, 1\}^k \times \{0, 1\}^\ell \rightarrow \{0, 1\}^\ell$ be a blockcipher. Given a kr-adversary $B$ making $q$ (distinct!) oracle queries, we can construct a PRF adversary $A$ making $q$ oracle queries such that

$$\text{Adv}^\text{kr}_E(B) \leq \text{Adv}^\text{prf}_E(A) + 2^{k-q\ell}.$$ 

The running time of $A$ is that of $B$ plus $O(q\ell)$.

**Interpretation:**

$E$ is PRF secure $\Rightarrow \text{Adv}^\text{prf}_E(A)$ is small $\Rightarrow \text{Adv}^\text{kr}_E(B)$ is small $\Rightarrow E$ is KR-secure.

**Example:** If $E = AES$ and $q = 2$ then $2^{k-q\ell} = 2^{-128}$.

Our first example of a reduction and a proof by reduction!
Game defining kr-advantage of an adversary $B$ against $E$

**Game $\text{KR}_E$**

**procedure Initialize**

$K \leftarrow \{0, 1\}^k$; $i \leftarrow 0$

**procedure $\text{Fn}(M)$**

$i \leftarrow i + 1$; $M_i \leftarrow M$

$C_i \leftarrow E(K, M_i)$; Return $C_i$

**procedure Finalize($K'$)**

$\text{win} \leftarrow \text{true}$

For $j = 1, \ldots, i$ do

If $E(K', M_i) \neq C_i$ then $\text{win} \leftarrow \text{false}$

Return $\text{win}$

The kr-advantage of $B$ is

$$\text{Adv}_E^{\text{kr}}(B) = \Pr[\text{KR}_E^B \Rightarrow \text{true}]$$
Games defining prf-advantage of an adversary $A$ against $E$

**Game $Real_F$**

**procedure Initialize**

$K \leftarrow \{0, 1\}^k$

**procedure $Fn(M)$**

Return $E(K, M)$

**Game $Rand_{\{0,1\}^\ell}$**

**procedure $Fn(M)$**

if $T[M] = \bot$ then $T[M] \leftarrow \{0, 1\}^\ell$

Return $T[M]$

The prf-advantage of $A$ is

$$Adv^\text{prf}_E(A) = \Pr[Real^A_E \Rightarrow 1] - \Pr[Rand^A_{\{0,1\}^\ell} \Rightarrow 1]$$
Proof of Proposition

Given $B$ we build $A$ as follows:

\[
\begin{align*}
\textbf{adversary } A \quad & \\
i & \leftarrow 0; \quad d \leftarrow 1 \\
K' & \leftarrow B^{\text{FnKRSim}} \\
\text{For } j = 1, \ldots, i \text{ do} \\
& \quad \text{If } (E(K', M_j) \neq C_j) \text{ then } d \leftarrow 0 \\
\text{Return } d 
\end{align*}
\]

\[
\begin{align*}
\textbf{subroutine } \text{FnKRSim}(M) \quad & \\
i & \leftarrow i + 1; \quad M_i \leftarrow M \\
C_i & \leftarrow \text{Fn}(M_i) \\
\text{return } C_i 
\end{align*}
\]

$A$ runs $B$, simulating $B$’s oracle via a subroutine that in turn invokes $A$’s own $\text{Fn}$ oracle. When $B$ returns a key $K'$, adversary $A$ returns 1 if $K'$ is consistent with the input-output examples, and 0 otherwise.
Real game analysis

Game $\text{Real}_E$

**procedure Initialize**

$K \leftarrow \{0, 1\}^k$

**procedure $\text{Fn}(M)$**

Return $E_K(M)$

When $A$ is executed in game $\text{Real}_E$, subroutine $\text{FnKRSim}(M)$ will return $\text{Fn}(M)$, which equals $E_K(M)$.

So $B$ is getting the same responses it would in game $\text{KR}_E$.

So $K'$ will be consistent with $(M_1, C_1), \ldots, (M_q, C_q)$ with probability the kr-advantage of $B$.

So

$$\Pr \left[ \text{Real}_E^A \Rightarrow 1 \right] = \text{Adv}^{kr}_E(B).$$
Rand game analysis

```
Game Rand_{0,1}^\ell

procedure Fn(x)
    if T[M] = ⊥ then T[M] ← $ \{0, 1\}^\ell$
    Return T[M]
```

When $A$ is executed in game $\text{Rand}_{0,1}^\ell$, subroutine $\text{FnKRSim}(M)$ will return $\text{Fn}(M)$, which is a random $\ell$-bit string.

So $B$ is getting back a sequence of $q$ random, independent $\ell$-bit strings.

So $K'$ will be consistent with $(M_1, C_1), \dotsc, (M_q, C_q)$ with probability at most $2^k/2^{q\ell}$, because there are $2^k$ choices for $K'$ and $2^{q\ell}$ choices for $(C_1, \dotsc, C_q)$.

So

$$\Pr \left[ \text{Real}_E^A \Rightarrow 1 \right] \leq 2^{k-q\ell}.$$
There is a lot going on in this proof! Look over it slowly, checking each step. In particular:

So $K'$ will be consistent with $(M_1, C_1), \ldots, (M_q, C_q)$ with probability at most $2^k/2^{q\ell}$, because there are $2^k$ choices for $K'$ and $2^{q\ell}$ choices for $(C_1, \ldots, C_q)$.

This is subtle because $B$ picks $K'$ as a function of $C_1, \ldots, C_q$. The claim is justified by a counting argument. There are $2^{q\ell}$ sequences $(C_1, \ldots, C_q)$, but for only $2^k$ of them does there even exist a $K'$ which is consistent with $(M_1, C_1), \ldots, (M_q, C_q)$.

We will do many such proofs, and you will be asked to do them on quizzes, so spend the time to understand this one! Ask now if you have doubts!
Our Assumptions

DES, AES are good block ciphers in the sense that they are PRF-secure up to the inherent limitations of the birthday attack and known key-recovery attacks.

You can assume this in designs and analyses.

But beware that the future may prove these assumptions wrong!
Exercise: Setup

Let $F : \{0,1\}^k \times \{0,1\}^l \rightarrow \{0,1\}^L$ be a family of functions where $l, L \geq 128$. Consider the following game $G$:

```plaintext
procedure Initialize
\[ K \leftarrow \{0,1\}^k \; ; \; b \leftarrow \{0,1\} \]

procedure LR($x_0, x_1$)
\[ \text{Ret } F(K, x_b) \]

procedure Finalize($b'$)
\[ \text{Ret } (b = b') \]
```

We define

$$\text{Adv}_{F}^{lr}(B) = 2 \cdot \Pr \left[ G^B \Rightarrow \text{true} \right] - 1.$$ 

Let $(x_0^1, x_1^1), \ldots, (x_0^q, x_1^q)$ be the queries that $B$ makes to its oracle. (Each query is a pair of $l$-bit strings, and there are $q$ queries in all.) We say that $B$ is legitimate if $x_0^1, \ldots, x_0^q$ are all distinct, and also $x_1^1, \ldots, x_1^q$ are all distinct. We say that $F$ is LR-secure if $\text{Adv}_{F}^{lr}(B)$ is “small” for every legitimate $B$ of “practical” resources.
Exercise: Questions

1. Show that the legitimacy condition is necessary for LR-security to be “interesting” by showing that if $F$ is a block cipher then there is an efficient, illegitimate $B$ such that $\text{Adv}^\text{lr}_F(B) = 1$.

2. Let $B$ be a legitimate lr-adversary that makes $q$ oracle queries and has time-complexity $t$. Specify a prf-adversary $A$, also making $q$ oracle queries and having time-complexity close to $t$, such that

$$\text{Adv}^\text{lr}_F(B) \leq 2 \cdot \text{Adv}^\text{prf}_F(A).$$

Explain why this reduction shows that if $F$ is a secure PRF then it is LR-secure.

3. Is the converse true? Namely, if $F$ is LR-secure, then is it a secure PRF? Answer YES or NO. If you say YES, justify this via a reduction, and, if NO, via a counter-example.