Birthday bound $\approx \dfrac{q^2}{N}$ The probability that q random values from a domain size N has at least one respected pair.

$$\Pr[\text{choice } 1 \text{ matches a prior choice}] = 0$$
$$\text{" " } 2 \text{ " " " "}] = \frac{1}{N}$$
$$\text{" " } 3 \text{ " " " "}] \leq \frac{2}{N}$$
$$\text{" " } 4 \text{ " " " "}] \leq \frac{3}{N}$$
$$\text{" " } q \text{ " " " "}] \leq \frac{q-1}{N}$$

Summation

$$\Pr[\text{any of the first } q \text{ choices match}] \leq \Sigma = \frac{q(q-1)}{2N}$$

Birthday Bound is an upper bound $< \dfrac{q^2}{N}$

Distinguishing: Block cipher vs. random permutation

Security bounds: range of possible attack advantages.

- lower bounds: an attacker can achieve at least this much. Show via an attack
- upper bounds: no attacker can do better than this.

Lower bound on Block cipher vs. random permutation

Let $E: \{0,1\}^k \to (\{0,1\}^b \to \{0,1\}^b)$ be a block cipher

World 1

k = random k bits

$f = E_k$

World 2

$f = \{0,1\}^b \to \{0,1\}^b$ random perm

Brute Force: Try all possible

Distinguish (f):

$x_0 = f(\langle 0 \rangle)$

$x_1 = f(\langle 1 \rangle)$

for $i = 1$ to t

if $(x_0 = E_{\langle i \rangle}(\langle 0 \rangle)$ and $x_1 = E_{\langle i \rangle}(\langle 1 \rangle))$

output "block cipher"

output "random perm"

Advantage = Pr[output block cipher | f is block cipher]

− Pr[output block cipher | f is random perm]

percentage of keys tried over t time

$$= \frac{t}{2^k} - \left(\frac{1}{2^b} \times \frac{1}{2^b}\right)t$$

$$= \frac{t}{2^k} - \frac{t}{2^{2b}}$$

$$= t\left(\frac{1}{2^k} - \frac{1}{2^{2b}}\right)$$

Much smaller than $\frac{1}{2^k}$

$$\boxed{\text{Advantage} \approx \frac{t}{2^k}}$$

lower bound on Block Cipher Security : $\frac{t}{2^k}$

upper bound on Block Cipher Security : ??? ε

// Unknown placeholder for unknown upper bound.

Assume to be $\approx \frac{t}{2^k}$ for a good block cipher

Distinguishing: Block cipher vs. random function

Block cipher   random perm   random func

$\frac{t}{2^k}$ $\frac{q}{2^b}$

$$\boxed{\frac{t}{2^k} + \frac{q}{2^b}}$$

t   Time spent offline in key search

q   # of black box invocations

Upper bound on CTR encryption: no adversary can do better

* Proven via "reduction"

Let f be either a block cipher with random key or a random function

BCDistinguisher (f)

let g = CTR encryption using f

if Real or Random Distinguisher (g) = "real"

output "block cipher"

else

output "random function"

A Reduction

If RRDist exist, then BCDist exists

Note: if f is a block cipher, then g is exactly CTR mode

if f is a random function, then g output uniform random bits

These are the two worlds a real or random distinguisher looks as.

if BCDistinguisher adv $< x$, then RRDistinguisher adv $< x$

BCDistinguish advantage $< \frac{t}{2^k} + \frac{q}{2^b}$

so RRDistinguisher adv $< \frac{t}{2^k} + \frac{q}{2^b}$

* Reductions will not be studied in this class