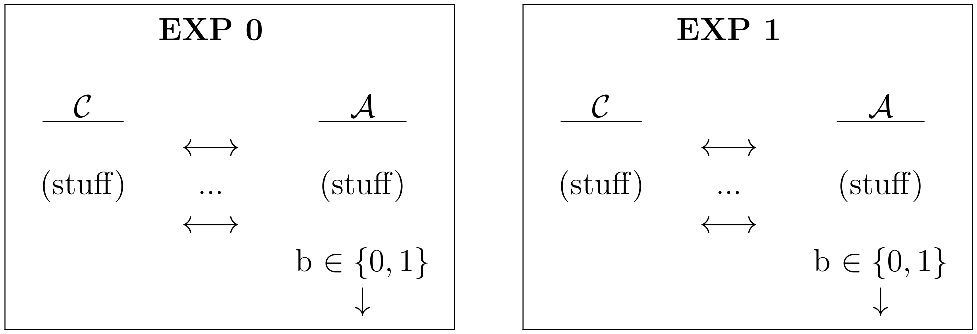


Recall the setup for a security game:

- A challenger $\mathcal{C}$ challenges an adversary $\mathcal{A}$.
- There are two possible versions of the game that we may be in:
  - **EXP 0** ("Experiment 0")
  - **EXP 1** ("Experiment 1")

  $\mathcal{C}$ knows which one we're in, but $\mathcal{A}$ doesn't.
- At the end of the game, $\mathcal{A}$ has to output a value $b \in \{0, 1\}$. (This is essentially a "guess" for which experiment they're in.)

We have the following definition of advantage for each game:

$$Adv_0\Big[\mathcal{A}\Big] = Pr\Big[\mathcal{A} \text{ outputs 0 in EXP 0}\Big] - \frac{1}{2}$$
$$Adv_1\Big[\mathcal{A}\Big] = Pr\Big[\mathcal{A} \text{ outputs 1 in EXP 1}\Big] - \frac{1}{2}$$

The overall advantage for the game is:

$$Adv[\mathcal{A}] = Adv_0[\mathcal{A}] + Adv_1[\mathcal{A}]$$

(Keep in mind that the definition of $Adv_0$ for a given adversary has absolutely nothing to do with **EXP 1** (and vice-versa). When you're calculating $Adv_0$, only look at the definition of **EXP 0** and the strategy (algorithm) of $\mathcal{A}$.)

**EXP 0**

$$\frac{\mathcal{C}}{c \xleftarrow{R} \{H, T\}} \quad \rightarrow \quad \frac{\mathcal{A}}{\ } \quad b \in \{0,1\} \downarrow$$

**EXP 1**

$$\frac{\mathcal{C}}{c = H} \quad \rightarrow \quad \frac{\mathcal{A}}{\ } \quad b \in \{0,1\} \downarrow$$

# 1

## 1.1

Recall the coin toss game. The challenger $\mathcal{C}$ sends the adversary $\mathcal{A}$ either HEADS or TAILS. Depending on the experiment, $\mathcal{C}$ either [uses a coin toss to decide], or [always sends HEADS].

Show the computation of the advantage of each of the following adversaries:

- $\mathcal{A}_1$: Always output $b = 1$.
- $\mathcal{A}_2$: Ignore the result reported by the challenger, and randomly output $b = 0$ or $b = 1$ with even probability.
- $\mathcal{A}_3$: Output $b = 1$ if HEADS was received, else output $b = 0$.
- $\mathcal{A}_4$: Output $b = 0$ if HEADS was received, else output $b = 1$.
- $\mathcal{A}_5$: If HEADS was received, output $b = 1$. If TAILS was received, randomly output $b = 0$ or $b = 1$ with even probability.

[SOLUTION:

- $Adv[\mathcal{A}_1] = (-1/2) + (1/2) = 0$
- $Adv[\mathcal{A}_2] = (0) + (0) = 0$
- $Adv[\mathcal{A}_3] = (0) + (1/2) = 1/2$
- $Adv[\mathcal{A}_4] = (0) + (-1/2) = -(1/2)$
- $Adv[\mathcal{A}_5] = (-1/4) + (1/2) = 1/4$

]

## 1.2

Play the game a few times, using these adversaries (or your own choice of strategy for the adversary)

# 2

Let's continue with the coin toss game from problem 1.

The strategy for $\mathcal{A}$ can be summarized using two probabilities, $h_0$ and $t_0$:

- When receiving $HEADS$:
  - Output $b = 0$ with probability $h_0$.
  - Else output $b = 1$.
- When receiving $TAILS$:
  - Output $b = 0$ with probability $t_0$.
  - Else output $b = 1$.

## 2.1

Why does this describe every possible adversary? (Assume $\mathcal{A}$ is an algorithm, although it may be randomized.)

## 2.2

Calculate the advantage of this general adversary in terms of $h_0$ and $t_0$.

## 2.3

What is the optimal strategy for $\mathcal{A}$? Prove that no other strategy can do better.

## 2.4

Prove that any adversary that ignores the information from the challenger has advantage 0.

# 3

## 3.1

Redo problems 1 and 2, with a modification to EXP 0: the challenger picks HEADS with probability 1/3 and TAILS with probability 2/3.

[SOLUTION:

- $Adv[\mathcal{A}_1] = (-1/2) + (1/2) = 0$
- $Adv[\mathcal{A}_2] = (0) + (0) = 0$
- $Adv[\mathcal{A}_3] = (1/6) + (1/2) = 2/3$
- $Adv[\mathcal{A}_4] = (-1/6) + (-1/2) = -(2/3)$
- $Adv[\mathcal{A}_5] = (-1/6) + (1/2) = 1/3$

]

## 3.2

What if you replace 1/3 with a variable probability $p$ (with $0 \leq p \leq 1$)?

[SOLUTION:

- $Adv[\mathcal{A}_1] = (-(1/2)) + (1/2) = 0$
- $Adv[\mathcal{A}_2] = (0) + (0) = 0$
- $Adv[\mathcal{A}_3] = (1/2 - p) + (1/2) = 1 - p$
- $Adv[\mathcal{A}_4] = (-(1/2) + p) + (-(1/2)) = -1 + p$
- $Adv[\mathcal{A}_5] = (-(p/2)) + (1/2) = (1 - p)/2$

]

# 4 Modular Factorial

Show that

$$(n-1)! \equiv -1 (\text{mod } n) \Leftrightarrow n \in \mathbb{P}$$

for $n > 4$. This is called Wilson's Theorem.

(Hint: First show that this equals 0 for any even number. Then show that it holds for a prime by using a generator to find which elements are inverses of another.)

[SOLUTION:

# 5 Coin Toss Game

[SOLUTION: Will have to simplify, maybe a lot, based on how class goes.]

Let's consider what it means for particular adversary to have a certain advantage, by considering a simple coin toss game where the adversary must distinguish a biased coin from a real one. In effect, we are computing how "defective" the biased coin is compared to a fair random number generator by how easily we can tell it apart.

We have two coins, a fair coin (probability $1/2$ of HEADS, otherwise TAILS), and a coin biased towards heads (probability $p$ of HEADS, otherwise TAILS, where $p > 1/2$). You may assume that the challenger and the adversary know $p$ ahead of time. To start the game, the challenger tosses a coin, as follows:

- In Experiment 0: The challenger tosses the fair coin.
- In Experiment 1: The challenger tosses the biased coin.

In both experiments, the challenger then sends the result of the toss to the adversary.

1. In the last step of each experiment, what does the adversary output, and why?
2. Let $\mathcal{A}$ be an adversary that outputs $\mathcal{A}(b)$ in Experiment $b \in \{0, 1\}$. Define the advantage of $\mathcal{A}$ (similar to the advantage for semantic security), and explain what it means.

3. What is the best possible advantage in this game? (Give a proof.)

1. The adversary outputs either 0 or 1. (S)he does this because (s)he is trying to determine which experiment (s)he is in. Being in Experiment 0/1 corresponds to having a fair/biased coin, so the output is effectively a guess for which coin was tossed.

2. The advantage is computes how good an adversary's guess is that the coin is biased. It's the difference between how often the adversary *incorrectly* guesses that the coin is biased and how often (s)he *correctly* tells that it's biased:

$$Adv(\mathcal{A}) = \Big| Pr[\mathcal{A}(0) = 1] - Pr[\mathcal{A}(1) = 1] \Big|$$

3. 
   - $Adv(\mathcal{A}_1) = |1 - 1| = 0$
   - $Adv(\mathcal{A}_2) = |1/2 - 1/2| = 0$
   - $Adv(\mathcal{A}_3) = |1/2 - p| = p - 1/2$
   - $Adv(\mathcal{A}_4) = |p - 1/2| = p - 1/2$
   - $Adv(\mathcal{A}_4) = |3/4 - (p + \frac{1}{2}(1 - p))| = p/2 - 1/4$

   Note that any adversary that ignores the information from the coin toss has advantage 0.

4. $\mathcal{A}_3$ and $\mathcal{A}_4$ have the optimal advantage, $p - 1/2$.

   Let $X \in \{H, T\}$ be the outcome of the toss reported by the challenger to the adversary (either HEADS or TAILS). The adversary has no information other than $X$ to distinguish the experiments, so we can define:

$$f(x) = Pr[\mathcal{A}(\cdot) = 1 \mid X = x]$$

   $f$ is effectively the probability our strategy guesses "biased" (Experiment 1) in each case. We can split the probability into cases based on $X$:

$$Adv(\mathcal{A}) = \Big| \Big(\frac{1}{2} f(H) + \frac{1}{2} f(T)\Big) - \Big(p \cdot f(H) + (1 - p) \cdot f(T)\Big) \Big|$$

$$= \Big| \Big(\frac{1}{2} - (1 - p)\Big) f(T) - \Big(p - \frac{1}{2}\Big) f(H) \Big|$$

$$= \left(p - \frac{1}{2}\right) \cdot \Big| f(T) - f(H) \Big|$$

The best strategy is to make sure the output is as different as possible depending on $X$. We could select $f(T) = 0$ and $f(H) = 1$, which corresponds to the strategy of adversary $\mathcal{A}_3$. (The opposite choice gives us $\mathcal{A}_4$).

]