Homework #2

Question 2.1

Show that $\frac{1}{p(n)} + \mu(n)$ is non-negligible

1. $\mu(n) + \frac{1}{p(n)} > \frac{1}{p(n)}$

2. Since $\frac{1}{p(n)}$ is non-negligible so is $\mu(n) + \frac{1}{p(n)}$

Question 2.1

Show that $\frac{1}{p(n)} - \mu(n)$ is non-negligible

1. $\mu(n) \in O(\frac{1}{2 * p(n)})$

2. $\exists n' \; \forall \; m > n' : \frac{1}{2 * p(m)} > \mu(m)$

3. $\exists n' \; \forall \; m > n' : \frac{1}{p(m)} - \mu(m) > \frac{1}{2p(m)}$

4. $\frac{1}{p(n)} - \mu(n) \in O(1/p(n))$

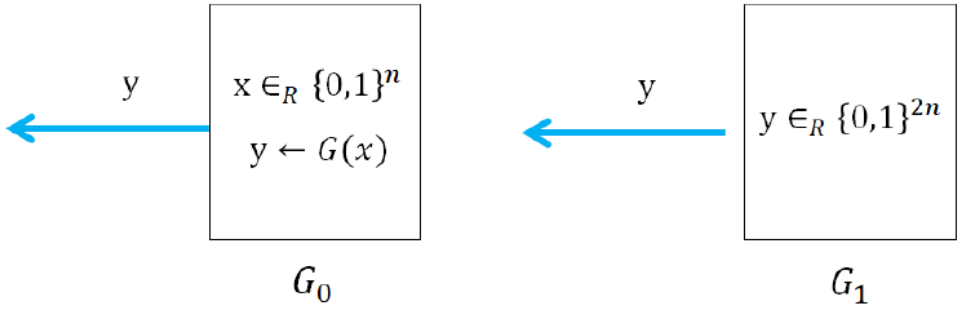
Question 2.2

- Show that p(n) * $\mu(n)$ is negligible

1. $p(n)$ is polynomial $\Rightarrow \exists\ c \in N$ such that $p(n) \in O(n^c)$
2. $\mu(n)$ is negligible $\Rightarrow\ \ \forall\ d \in N,\ \ \mu(n) \in O(n^{-d})$
3. $\forall\ d \in N,\ p(n) \cdot \mu(n)\ \in O(n^{c-d})$
4. $\forall\ e \in N,\ p(n) \cdot \mu(n)\ \in O(n^{-e})$
5. Step 4 is equivalent to saying that $p(n) \cdot \mu(n)$ is negligible

Question 3

3. Show that if $G : \{0,1\}^n \to \{0,1\}^{2n}$ is easy to invert (as defined below) then it is not a PRG. Do this by constructing a distinguisher D which distinguisher between G_0 and G_1. In more formal terms, construct a distinguisher D such that $|\Pr[D(G_1) = 1] - \Pr[D(G_0) = 1]| \geq 1/p(n)$ for some polynomial p.

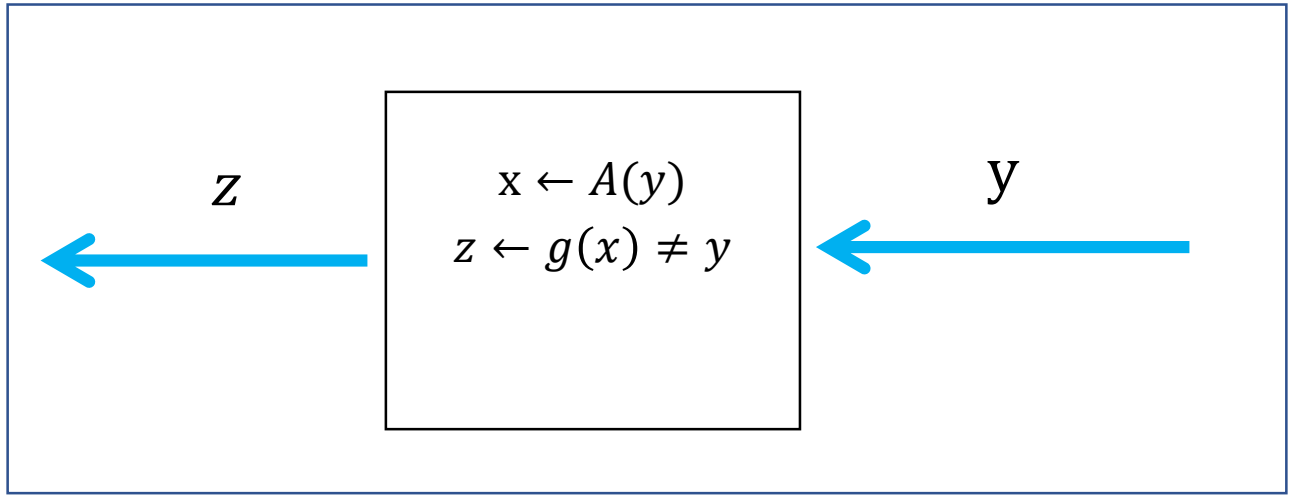


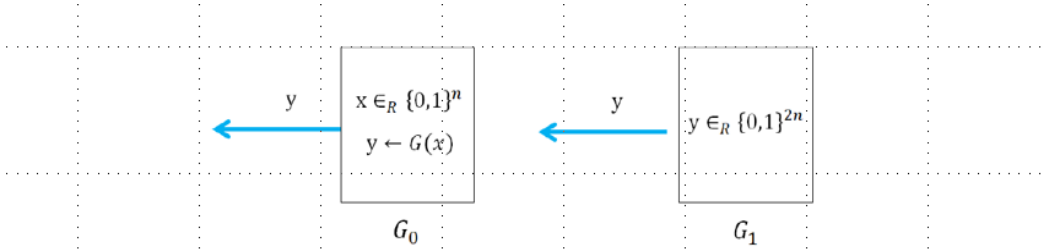
Definition 1. *We say that* $G : \{0,1\}^n \to \{0,1\}^{2n}$ *is easy to invert if there exists a probabilistic polynomial time algorithm* A*, polynomial* p *such that*

$$\Pr[A(y) = x \mid y \leftarrow G(x),\ x \in_R \{0,1\}^n] \geq 1/p(n)$$

Question 3

- Description of distinguisher



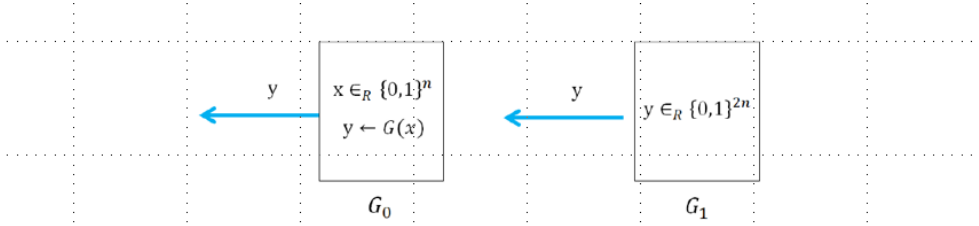


Definition 1. *We say that* $G : \{0,1\}^n \to \{0,1\}^{2n}$ *is easy to invert if there exists a probabilistic polynomial time algorithm* A*, polynomial* p *such that*

$$\Pr[A(y) = x \mid y \leftarrow G(x),\ x \in_R \{0,1\}^n] \geq 1/p(n)$$

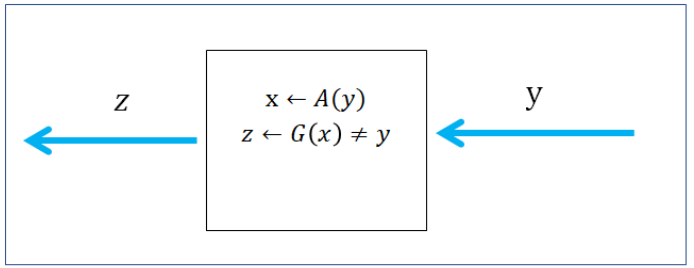
Question 3

- $\Pr[D(G_0) = 1)] \leq 1 - 1/p(n)$
  - $D(G_0) = 0$ only when $g(A(y)) = y$
  - $\Pr[g(A(y)) = y] \geq 1/p(n)$
  - $\Pr[D(G_0) = 0] \geq 1/p(n)$
  - $\Pr[D(G_0) = 1] \leq 1 - 1/p(n)$



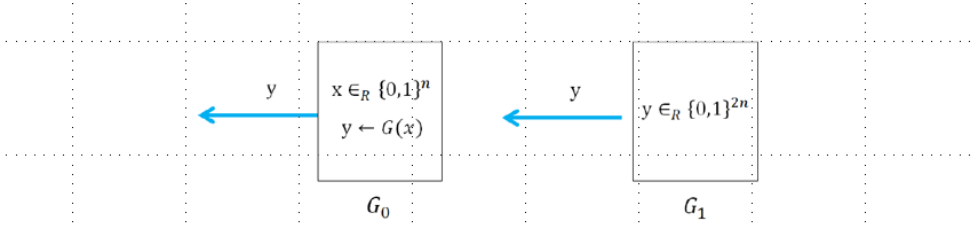
Definition 1. *We say that $G : \{0,1\}^n \to \{0,1\}^{2n}$ is easy to invert if there exists a probabilistic polynomial time algorithm A, polynomial p such that*

$$\Pr[A(y) = x \mid y \leftarrow G(x),\ x \in_R \{0,1\}^n] \geq 1/p(n)$$



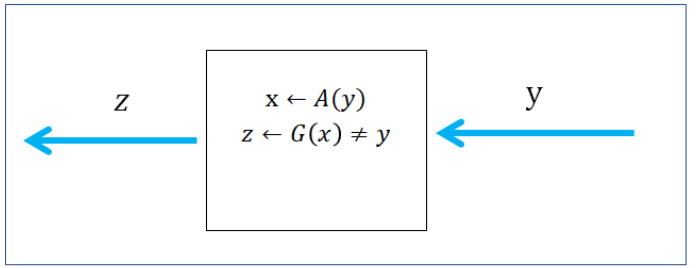
Question 3

- $\Pr[D(G_1) = 1)] \geq 1 - 1/2^n$
  - $D(G_1) = 0$ only when $g(A(y)) = y$
  - $\Pr[g(A(y)) = y] \leq \Pr[g^{-1}(y) \neq \perp]$
  - $\Pr[g^{-1}(y) \neq \perp] \leq 2^{-n}$
  - $\Pr[D(G_1) = 0] \leq 2^{-n}$
  - $\Pr[D(G_1) = 1] \geq 1 - 2^{-n}$



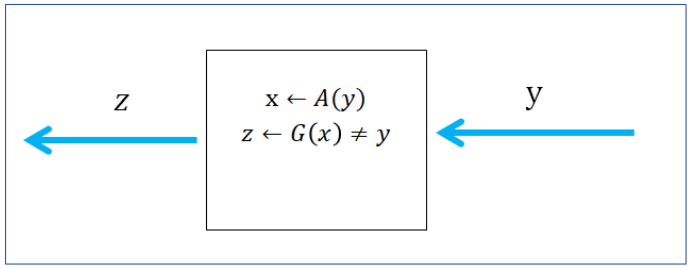
Definition 1. *We say that $G : \{0,1\}^n \to \{0,1\}^{2n}$ is easy to invert if there exists a probabilistic polynomial time algorithm A, polynomial p such that*

$$\Pr[A(y) = x \mid y \leftarrow G(x),\ x \in_R \{0,1\}^n] \geq 1/p(n)$$

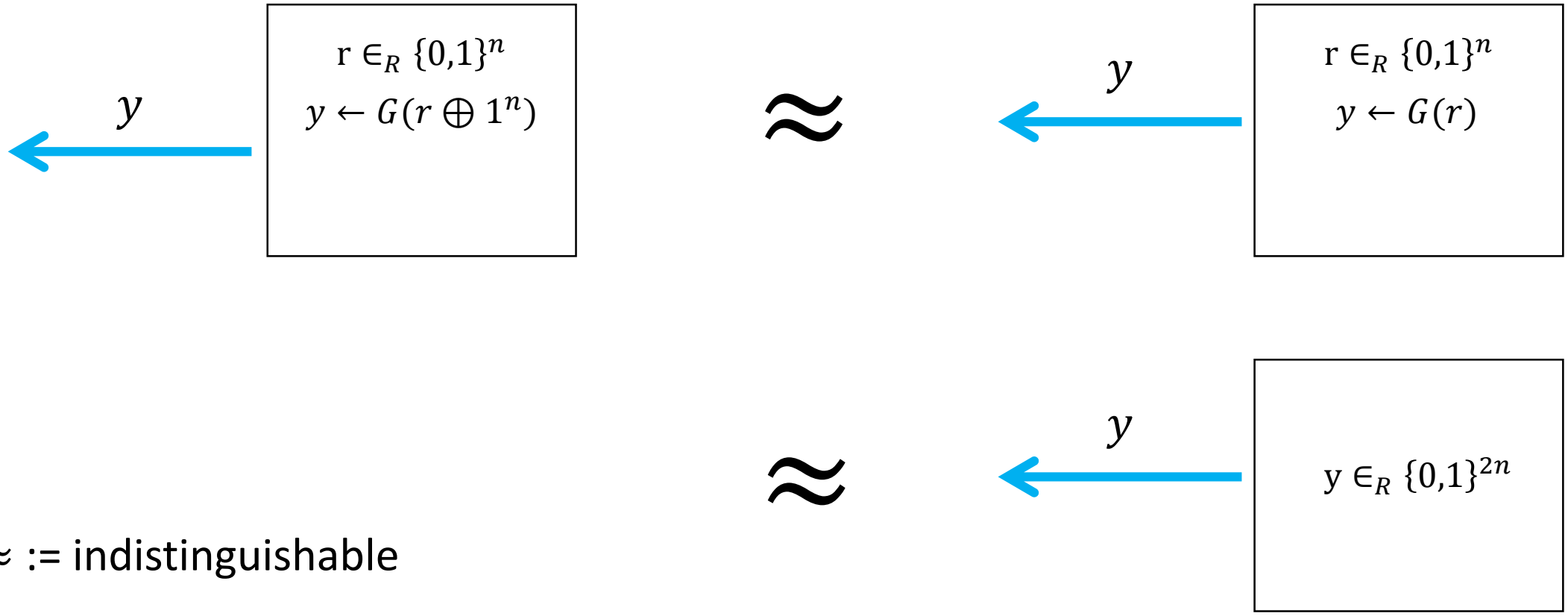


Question 3

- $\Pr[D(G_0) = 1)] \leq 1 - 1/p(n)$
- $\Pr[D(G_1) = 1)] \geq 1 - 1/2^n$
- $|\Pr[D(G_1) = 1)] - \Pr[D(G_0) = 1)| \geq 1 - 1/2^n - (1 - 1/p(n))$
- $|\Pr[D(G_1) = 1)] - \Pr[D(G_0) = 1)| \geq 1/p(n) - 1/2^n$
- $|\Pr[D(G_1) = 1)] - \Pr[D(G_0) = 1)| \geq \frac{1}{2 \cdot p(n)}$
- g is not a pseudo-random generator



$G'(r) := G(r \oplus 1^n)$ *is a PRG*



$\approx$:= indistinguishable

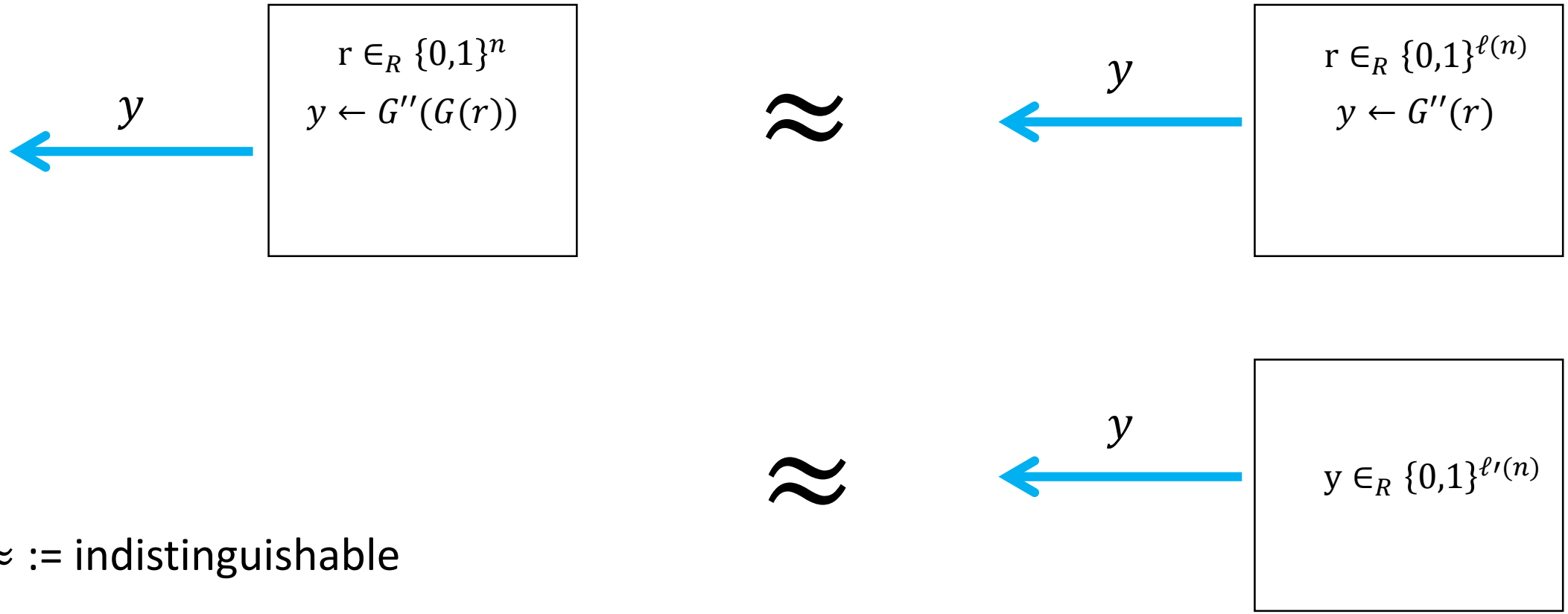
$G'(r) \coloneqq G(r) \oplus G(r \oplus 1^n)$ is not a PRG

1. $G(b||r') \coloneqq b \,||\, G''(r')$ is also a PRG when G'' is a PRG
2. $G'(b||r') \coloneqq (b \,||\, G''(r')\ ) \oplus \big((b \oplus 1) \,||\, G''(r' \oplus 1^{n-1})\big)$
3. $G'(b||r') \coloneqq \big(b \oplus b \oplus 1) \,||\, G''(r')\ \oplus G''(r' \oplus 1^{n-1})\big)$
4. $G'(b||r') \coloneqq 1 \,||\, G''(r') \oplus G''(r' \oplus 1^{n-1})$
5. First bit of output is always 1 not random at all.

$G'(r)$ defined as the first $\ell(n) - 1$ bits of $G(r)$

- $G'(r)$ defined as the first $\ell(n) - 1$ bits of $G(r)$
  - Is always pseudo-random (always is indistinguishable from random)
  - If $\ell(n) = n + 1$
    - Input size is the same as the output size
    - Therefore does not have the expansion property

$G'(r) := G''(G(r))$ *where* G'' *is also a PRG*



≈ := indistinguishable

Question 5

- M={1100,0110,1001}

- $1100 \oplus 0110 = 1010$
- $1010 \oplus 1001 = 0101$

- If we xor 1010 to the ciphertext
  - If $m \in \{1100,0110\}$, the validation oracle will return accept
  - If $m = 1001$, the validation oracle will return reject

Question 6

- Validation oracle always accepts since all messages are valid

Question 3.9

- Construct a pseudo-random function
  - Input length log(n)
  - Key-length n
- $2^{\log n} = n$
- Function that takes log n bits and produces a single random output bit
- For each input, choose a random output bit
  - Since there are only n possible inputs, you can get a single output

Question 8

Forge a mac tag when p=183 and (m,t) = (0,53)

- $183 = 3 \cdot 61$
- $(m, t) = (0,53)$
- $(m', t') \leftarrow (61,53)$
- 61*k + t = t (mod 183) when $k \,\%\, 3 = 0$

Is $F'_k(x) := F_k(0 \,||\, x) || \, F_k(1||x)$ PRF?

- Yes, because an adversary in a PRF can choose inputs of his choice
  - In particular, he can sample x and query both
    - $0 \,||\, x$
    - $1 \,||\, x$

$F'_k(x) \coloneqq F_k(0 \,||\, x)|| \, F_k(x||1)$ is not a PRF?

- Choose x such that $(0 \,||\, x) = (x||1)$
- Denote $x' \coloneqq \ (0 \,||\, x) = (x||1)$
- $F'_k(x) = F_k(0 \,||\, x)|| \, F_k(x||1) = F_k(x')|| \, F_k(x') = (c, c)$

Show that Ax+b (mod 2) is not a pseudo-random function

- Construct an (A,b) as follows
  - $b = f(x_0)$ where $x_0 = (0, \ldots, 0)$
  - $A_i := f(x_i) \oplus b$ where $x_i = 0^i \,||1\,||\, 0^{n-i-1}$
- Sample a random $x_i \in \{0,1\}^n$
- Test if $Ax + b \neq f(x)$
  - Output "random" if $Ax + b \neq f(x)$
  - Output "pseudo-random" if $\mathrm{Ax} + \mathrm{b} = f(x)$

Question 3.18

- Dec(c)
  - $\mathrm{r} \,||\, m \leftarrow\ f^{-1}(c)$
  - Output m

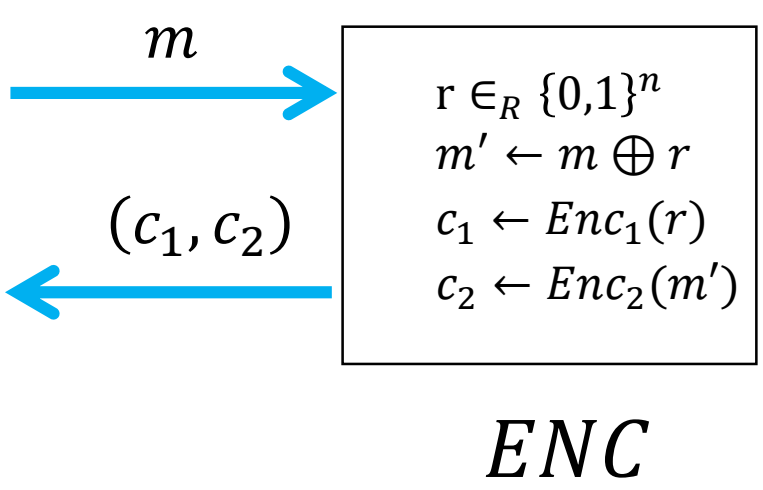
- Proof of security:
  - Step 1: Probability of collision that the same r is used is negligible
  - Step 2: Show that a distinguisher which breaks this scheme can also break the pseudo-random property of this scheme
    - Cannot distinguish which message was encrypted when Random function is used
    - If you could distinguish between the two, then you can distinguish between random and pseudo-random

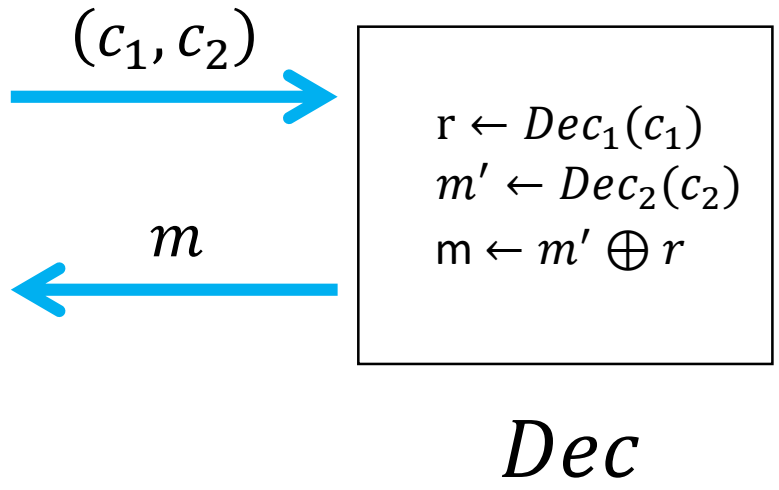
What happens with dropped blocks for CBC, OFB, CTR

- All blocks after dropped block decrypt incorrectly
- Possible to recover if you guess a block is missing for OFB and CTR

How to encrypt a message when one encryption scheme is insecure

- One-time pad is the key





Groups, fields, primes

Divisibility

- Definition: a divides n written as $(a \mid n)$ if there exists a number c such that $ca = n$

- $GCD(a, b) \coloneqq \max_{x \in \mathbb{N}} (x \mid a)\ and\ (x \mid b)$

Relatively prime

- We say that two numbers a, b are relatively prime (co-prime)

$$GCD(a, b) = 1$$

Examples

15,32

24, 35

Non-example

2,14

3, 183

Group

- A group
  - Consists
    - Set S
    - Operation $\odot : S \times S \rightarrow S$
    - Identity-element
  - Properties
    - Closure $x, y \in S \Rightarrow x \odot y \in S$
    - Identity $\exists\, e \in S : \; x \in S \Rightarrow e \odot x = x$ (we use e to denote the identity element)
    - Associativity $x, y, z \in S \Rightarrow (\mathrm{x} \odot y) \odot z \Rightarrow x \odot (y \odot z)$
    - Inverse: $x \in S \Rightarrow \exists\, y \in S : x \odot y = e$
  - Extra property
    - Commutativity: $x, y \in S \Rightarrow x \odot y = y \odot x$

Discrete logarithm

- Given group G, generator g, For a given y find x such
$$g^x = y$$

- Reminder g is a generator if $\{g^i \mid i \in N\} \coloneqq G$

- Cryptographers hope that in certain groups, finding discrete logarithm is hard.

Z_n^*

- $Z_n^* := \{x \in Z_n \mid GCD(x, n) = 1\}$
- $(Z_n^*, \times)$ is an abelian group when $\times$ denotes modular multiplication Z_n
- Going to be critical for many cryptosystems.

Z_6^*

- $Z_6^* := \{x \in Z_6 \mid GCD(x, 6) = 1\} = \{1,5\}$

Z_6^*

- $Z_6^* := \{x \in Z_6 \mid GCD(x, 6) = 1\} = \{1,5\}$

- The multiplicative inverse of x in Z_n

  $y \in Z_n$ such that $x \cdot y = 1 \ (mod\ n)$

- Inverses :
  - (1,1)
  - (5,5)

Z_6^*

- $Z_6^* := \{x \in Z_6 \mid GCD(x, 6) = 1\} = \{1,5\}$

- Group generated (power table)
  - $5 \rightarrow (5^1, 5^2) = (5,1)$ (5 is a generator of the group)
  - $1 \rightarrow 1$ (1 is not a generator)

- Inverses :
  - $(1,1)$
  - $(5,5)$

$(Z_7,*)$

- Multiplicative inverse
  - $(1,1)$
  - (2,4)
  - (3,5)
  - (6,6)

- Generator (power table)
  - $3 \rightarrow (3^1, 3^2, 3^3, 3^4, 3^5, 3^6, 3^7) = (3,2,6,4,5,1)$
  - $5 \rightarrow (5^1, 5^2, 5^3, 5^4, 5^5, 5^6, 5^7) = (5,4,6,2,3,1)$

Discrete logarithm

- Generator (power table)
  - $3 \rightarrow (3^1, 3^2, 3^3, 3^4, 3^5, 3^6, 3^7) = (3,2,6,4,5,1)$
  - $5 \rightarrow (5^1, 5^2, 5^3, 5^4, 5^5, 5^6, 5^7) = (5,4,6,2,3,1)$
- Log_3
  - $(1,2,3,4,5,6) \rightarrow (7,2,1,4,5,3)$
- Log_5
  - $(1,2,3,4,5,6) \rightarrow (7,4,5,2,1,6)$

Z_8^*

- $Z_8^* := \{x \in Z_8 \mid GCD(x, 8) = 1\} = \{1,3,5,7\}$

- The multiplicative inverse of x in Z_n

  $y \in Z_n$ such that $x \cdot y = 1 \ (mod\ n)$

- Inverses :
  - (1,1)
  - (3,3)
  - (5,5)
  - (7,7)

Z_8^*

- $Z_8^* := \{x \in Z_8 \mid GCD(x, 8) = 1\} = \{1,3,5,7\}$
- Subgroups of Z_8^* are either of size $1,2,4$
- Group generated
  - $1 \rightarrow \{1\}$
  - $3 \rightarrow \{3,1\}$
  - $5 \rightarrow \{5,1\}$
  - $7 \rightarrow \{7,1\}$
  - Z_8^* has no generators

Z_{15}^{*}

- $Z_{15}^{*} := \{x \in Z_{15} \mid GCD(x, 15) = 1\} = \{1,2,4,7,8,11,13,14\}$

- The multiplicative inverse of x in Z_n

  $y \in Z_n$ such that $x \cdot y = 1 \ (mod\ n)$

- Inverses :
  - (1,1)
  - (2,8)
  - (4,4)
  - (7,13)
  - (11,11)
  - (14,14)

Z_{15}^{*}

- $Z_{15}^{*} := \{x \in Z_{15} \mid GCD(x, 15) = 1\} = \{1,2,4,7,8,11,13,14\}$
- The multiplicative inverse of x in Z_n

  $y \in Z_n$ such that $x \cdot y = 1 \ (mod\ n)$
- Subgroups
  - (1,4,11,14) -> ({1},{4,1},{11,1},{14,14}}
  - 2 -> {2,4,8,1}
  - 8 -> {8,4,2,1}
  - 7 -> {7,4,13,1}
  - 13 -> (13,)

Examples of group

- $(Z_n \setminus \{0\},\ *)$ is a group if and only if n is prime

Field

- Field
  - Consists
    - Set S
    - Operations $(+,\times)$
    - Zero-element 0
    - One-element 1
  - Properties
    - $(S,+)$ is a *commutative* group with identity element 0 (inverse of a is $-a$)
    - $(S \setminus \{0\},\times)$ is a *commutative* group with identity element 1 (inverse of a is $a^{-1} = 1/a$)
    - Distributivity:

Arithmetic fields over (mod n)

- $(Z_n, +, *)$ is a field if and only if n is prime