45/50

CHENNAI MATHEMATICAL INSTITUTE
https://www.cmi.ac.in

Mid Semester Examination, Sep–Oct 2024

Name: Anitra	Roll Number: MCS202304
Date:	Subject: Crypto
Course & Year: 2024	Total No. of Pages:

We are using re-cycled paper for the internal exams. Please ignore the pre-printed matter on the sheets.

—— Begin writing from the next page ——

from next page

B1. Write your solution to B1 below.

2141

Answers to part B of 2024 Entrance Examination for BSc Programmes at CMI

- **Clearly explain your entire reasoning.** No credit will be given without correct reasoning. Partial solutions may get partial credit.
- **In problems with multiple parts**, you may solve a later part of a problem by assuming some previous part(s), even if you could not do the earlier part(s).

2. (a) $F'_K(x) = F_K(0x)\,F_K(x_0)$, $x \in \{0,1\}^{n+1}$

now let's observe the output for,

$$x = 0^{n+1}$$

$$F'_K(x) = F_K(0^n) \,||\, F_K(0^n)$$

So, distinguisher D given 0^{n+1} as input will check its output if $(L||R)$, check $L == R$ ✓

for a random function this will happen with probability $\frac{1}{2^n}$

PTO

(b) let x_1 be 01^{n-2}

x_2 be 1^{n-1}

Now, $F'_K(x_1) = F_K(001^{n-2}) F_K(01^{n-1})$

$F'_K(x_2) = F_K(01^{n-1}) F_K(1^n)$

now, distinguisher D on two outputs $L_1 \| R_1$ and $L_2 \| R_2$

will check.

if $L_2 == R_1$.

if the function used is F'_K then. $P_r(L_2 = R_1) = 1$

else it will be $= \frac{1}{2^n}$ (two n length string being equal

10

Blank page for rough work/continuation of part B solutions

(1) (b) let H be a PRG, s.t. $H: \{0,1\}^{n+1} \to \{0,1\}^{n^2}$. then PRG always exists by PRG length extension lemma which uses hybrid arg

now, let G be a following PRG,
(G on input $x = x_0 b$, $b \in \{0,1\}$ returns)
$G(x_0 b) = H(x_0)$

G does not really take input, it chooses one randomly. we are thinking of the random tape to simplify

now, $G(x_0 b)$ should be pseudorandomly distributed as H is a PRG.

but, in this case, $G'(s) = G(s)\,G(s+1)$

now, if the last bit of s is 0, ie $s = x_0 0$
SH will be of form $SH = x_0 1$

So, $G'(x_0 0) = G(x_0 0)\,G(x_0 1)$

$= H(x_0)\,H(x_0)$

So, distinguisher can check if the output L||R is in the form $L == R$, that case will happen with probability $1/2$ (last bit of s is 0 and it with req prob.)

if the string is random again $L = R$ will happen with probability $\frac{1}{2^n}$

(1)(a) G' is a PRG.

Proof: The intuition is that for any Distinguisher D,

let S_0 denote the subset of strings in $\{0,1\}^n$.

s.t. if $s \in S_0$, $D(G(s)) = 1$

if we randomly pick s from $\{0,1\}^n$

both s and $\bar{s}$ (complement) will have equal probability of being in S_0.

So. if s is random, then complementing it to get $\bar{s}$ is a overall random process.

10

now if a distinguisher D can distinguish between G' and U_{n2} then, D can distinguish between G' when G picks s and complement it. and U_{n2}.

But, as from the intuition complementation should not help a distinguisher. then D_{18} should be able to distinguish between G and U_{n2} contradicting G is a PRG.

3. (a) $f: \{0,1\} \to \{0,1\}^n$

$g: \{0,1\}^{3n} \to \{0,1\}^{3n}$

s.t. $g(a,b,c) = (b, c, a \oplus f(b))$

for, (a_1, b_1, c_1) and (a_2, b_2, c_2)

we can see, if $b_1 \neq b_2$

or $c_1 \neq c_2$

no way, $g(a_1, b_1, c_1) \neq g(a_2, b_2, c_2)$

but, even if $b_1 = b_2$, $c_1 = c_2$

a_1 must not be equal to a_2

and $f(b)$ are always same as $b_1 = b_2$.

so, $a_1 \oplus f(b) \neq a_2 \oplus f_b$ (as $a_1 \neq a_2$)

$\therefore$ if $(a_1, b_1, c_1) \neq (a_2, b_2, c_2)$

then $g(a_1, b_1, c_1) \neq g(a_2, b_2, c_2)$

as domain and range same, it's a bijection

Blank page for rough work/continuation of part B solutions

(3)(b) [redacted]

$\Rightarrow$ [redacted] F'_{K_1, K_2, K_3} is a permutation

Proof: using induction on number of rounds.

now, for round ①. if $(a, b, c)_1 \neq (a, b, c)_2$

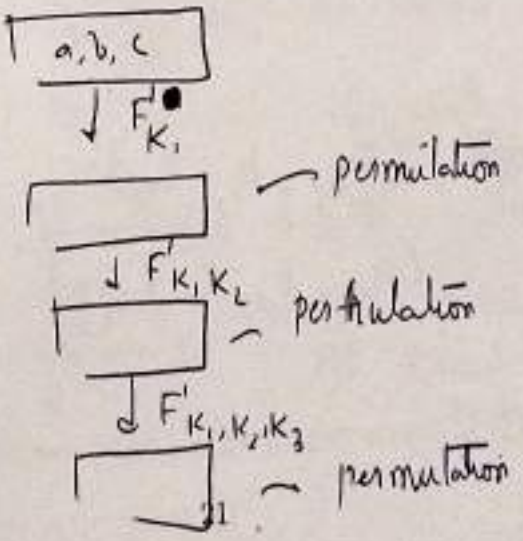
then. even if f is a function,

$(b, c, a \oplus f(b))$ is a permutation as

$F'_{K_1} : \{0,1\}^{3n} \rightarrow \{0,1\}^{3n}$ is a [redacted] bijection.

↳ propagating this logic for 2 more rounds.

we can say that, F''_{K_1, K_2, K_3} is a permutation.



(a) $F'_{K_1 K_2 K_3}$ is not a pseudorandom permutation

Let. consider two inputs (a_1, b_1, c_1) I_1

(a_1, b_1, c_2) I_2

Now, $F'_{K_1 K_2 K_3}(I_1) = (a_1 \oplus F_{K_1}(b_1),\ b_1 \oplus F_{K_2}(c),\ \ldots)$

L_1(left) M_1(Middle) R_1(Right)

$F'_{K_1 K_2 K_3}(I_2) = (L_2, M', \ldots R')$ then

So, distinguisher on input can check,

if $(L_1 = L_2)$

if the oracle is $F'_{K_1 K_2 K_3}$ then $P_r(L_1 = L_2) = 1$

else. $P_r(L_1 = L_2) = 1/2^n$.

Moreover, on inputs, (a_1, b_1, c_1) $L_1 \oplus L_2$ will give

(a_2, b_1, c_1) $a_1 \oplus a_2$

10

Solution to B5 continued

(4) let: $F: \{0,1\}^{2n} \times \{0,1\}^n \to \{0,1\}^n$

now, let the intended PRG be the following G,

$$G(x) = F_x(0) \| F_x(1) \| \dots \| F_x(n-1)$$
$$x \in \{0,1\}^{2n}$$

[redacted]

0, 1, ... n-1 encoded in $\{0,1\}^n$

Claim: G is a pseudo random generator.

Proof: { if f is a random [redacted] function, the output of G would be a completely random [redacted] string

{ if F_x is used, then the output of G will be $B_0 \| B_1 \| \dots \| B_{n-1}$ where all $B_0 \dots B_{n-1}$ are distinct.

(1) { But [redacted] as f is queried polynomially many times, the chance of collision will be negligibly small. which is $\leq \frac{\binom{n}{2}}{2^n} = \frac{n(n-1)}{2^{n+1}}$ (n blocks, each pair can be equal with prob $1/2^n$, so by union bound)

Solution to B5 continued in pages 14 to 28? Write the page number here ____

10

B6. Write your solution to B6 below.

Now if some distinguisher D can distinguish between output of G when G uses random function and PRPs then, we can modify it to get another distinguisher D' which can distinguish between F_x and f

let D' be the following distinguisher.

1) on input- x.

2) calls the oracle on 0, ... (n-1)

3) gets output $b = b_1 \ldots b_{n-1}$

4) call D on b

5) if D says { G is PRG, says oracle is F_x ; G is random, says oracle is f }

That is contradiction, as

1) we have shown that, for any distinguisher, by (1) it isn't possible to distinguish between a random function and a random permutation with polynomial advantage

2) for any random permutation and PRP, and distinguisher should have only polynomial advantage

{ So, if D exists, D' exists making the block cipher vulnerable }

Rough work

The $Dec'_K(c)$ works following way.

on input c { c has length $l(n) \cdot t(n)$ }

$Dec'_K(c)$ divides it into $t(n)$ equal parts (one block will have length $l(n)$)

now, $Dec'_K(c)$ runs

① $Dec_K(c_1)$ [redacted] b_1

to get, $r_1 b_1$ [redacted]

now, $Dec'_K(c)$ runs

② $Dec_{r_1}(c_2)$ b_2

to get $r_2 b_2$

this way $Dec'_K(c)$ gets back $b_1 b_2 \cdots b_{t(n)}$

5

Rough work

Let us define the following hybrids,

$$H_0 = Enc_k(r,b_1) \mid Enc_{r_1}(r_2,b_2) \mid \dots Enc_{r_{t(n)-1}}(r_{t(n)},b_n)$$

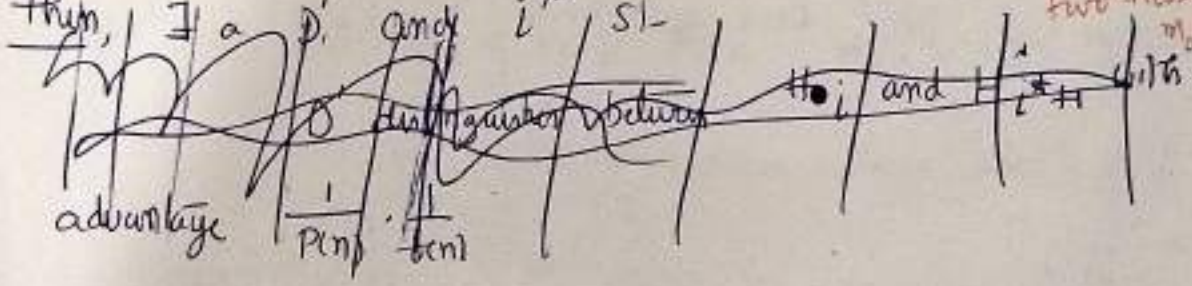
$$H_i = r'_{1(n)} \quad r'_{t(n)} \mid Enc_{r_{i+1}}(r_{i+2},b_2) \mid \dots$$

what are these?

$$H_{t(n)} = r'_{1(n)} \dots r'_{1(n)} \cdot r'_{t(n)}$$

now, if any distinguisher distinguishes between H_0 and $H_{t(n)}$ with probability advantage $\frac{1}{p(n)}$

The adv test is to dist. between two messages $m_0 \& m_1$



Let's try to prove why

$$Enc_k(r,b_1)\ Enc_{r_1}(r_2,b_2)$$ is pseudorandom

compared to $U_{2l(n)}$

Solution to B2 continued

Claim ① $Enc_K(r,b_1)\ Enc_{r_1}(r_2,b_1)$ is indistinguishable to $Enc_K(r,b_1)\ Enc_r(r_2,b_1)$ where $r \in_R \{0,1\}^n$

i.e $Enc_K(r,b_1)Enc_{r_1}(r_2,b_1) \approx_\varepsilon Enc_K(r,b_1)Enc_r(r_2,b_1)$

this is true because,

both r and r_1 are chosen randomly, and if we have replaced $Enc_K(r,b_1)$ with $Enc_K(r,b_1)$ it should not have any effect as Enc_K is EAV, secure

as $[Enc_K(r_1,b_1)\ Enc_r(r_2,b_2)] \approx_\varepsilon U_{2l(n)}$ negligible distance

Considering this, H_0 and H_2 should have negligible distance

H_2 and H_4 .. and similarly H_1 H_3, H_3 H_5 ...

~~this too~~ Also, H_0 and H_1 are indistinguishable from claim ①.

∴ all the hybrids are indistinguishable from each other making ↗ EAV-secure

Solution to B2 continued in pages 14 to 28? Write the page number here ____