CS:616 CRYPTOLOGY

PRACTICE QUESTIONS
LECTURE

Instructions

- Try these questions before tutorial next week.

(1) Let $G : \{0,1\} \ \rightarrow \{0,1\}^3$ be a secure length tripling PRG. For each function below state whether it is also a secure PRG. If the function is a secure PRG, give a proof. If not, then describe a successful distinguisher and give estimates on its advantage. When we write $a||b||c := G(s)$, each a, b, c have length .

(a) $H(s)$:

$$x||y||z := G(s)$$
$$\text{return } G(x)||G(z).$$

(b) $H(s)$:

$$x := G(s)$$
$$y := G(0\ )$$
$$\text{return } x||y$$

(c) $H(s)$:

$$x := G(s)$$
$$y := G(0\ )$$
$$\text{return } x \quad y$$

(2) Let G and G_2 be deterministic functions, each accepting inputs of length and producing outputs of length 3 . De ne the function $H(s\ ||s_2) = G\ (s\ )$ $G_2(s_2)$. Prove that if either of G or G_2 or both is a secure PRG then so is H.

(3) Let f be any function. Show that the following G is not a secure PRG, no matter what f is. Describe a succesful distinguisher and explicitly compute its advantage:

$G(s)$: return $s||f(s)$