

**CSCI 283 - Computer Security I - Fall 2003**  
**George Washington University**

**Cryptanalysis Examples II**

10 September 2003

A. Consider the following cryptosystem: the plaintext is a binary string of length  $n$ . The key is a binary string of the same length. Encryption is the XOR of the two strings. The probability of key bit being 1 is  $p$  and each key bit is independent of the other. For what values of  $p$  is the cipher unconditionally secure?

B. Consider a similar cryptosystem: the plaintext is a binary string of length  $n$ . The key is a binary string of the same length. Encryption is the XOR of the two strings. The key is computationally generated using a  $b$ -bit pseudo-random number generator (PRNG),  $b \ll n$ . Is the cipher unconditionally secure? Is it computationally secure?

C. Deduce the English plaintext corresponding to the following ciphertext. Assume that spaces have been retained:

lxr rwq zoazqgr sfuqb bqabq virw gxlkiz uqnb, vwqjq ir bIsgkn sqfab fggkniay rwq gjicfrq rjfab-  
mojsfrioa mijbr fad rwqa rwq gxlkiz oaq. wq wfec aorqd rwfr f sfej gjolkqs virw gjicfrq uqnb ib  
rwq bwqqj axslqj om uqnb f biaykq xbqj wfb ro brojq fad rjfzu. virw gxlkiz uqnb, oakn rvo uqnb  
fjq aqqdqd gjj xbqj: oaq gxlkiz fad oaq gjicfrq. Kqr xb bqq vwfr dimmejgazq rwib sfuqb ia rwq  
axslqj om uqnb aqqdqd.