

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

Cryptanalysis Examples II: Solutions

17 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?

Before one obtains the ciphertext, the message could be anything.

When $p > 0.5$, if one always guesses that the key bit is a 1 and determines the plaintext from the ciphertext using this assumption, one would be correct at least $p > 0.5$ of the time. This is better than not knowing anything about the plaintext. Hence the cipher is not unconditionally secure for $p > 0.5$.

Similarly, when $p < 0.5$, one can always guess that the key bit is a 0. The cipher is not unconditionally secure for $p < 0.5$.

When $p = 0.5$, one will be wrong half of the time whatever one guesses the key bit to be. This is no better than before knowing the ciphertext, hence the cipher is unconditionally secure only when $p = 0.5$.

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 seed for a pseudo-random number generator (PRNG), $b \ll n$. Is the cipher unconditionally secure? Is it computationally secure?

The cipher is not unconditionally secure because, before knowing the ciphertext, the plaintext could be any of 2^n strings. After knowing the ciphertext, as the number of possible key strings is only 2^b (one for each seed), the plaintext can only be one of 2^b strings.

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 rjfabmojsfria mijbr fad rwqa rwq gxlkiz oaq. wq wfcq aorqd rwfr f sfoej 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 gqj xbqj: oaq gxlkiz fad oaq gjicfrq. Kqr xb bqj vwfr dimmejzazq rwib sfuqb ia rwq axslqj om uqnb aqqdqd.

See presentation slide set.