CIS 5371 Cryptography

QUIZ 6 (5 minutes only)

This quiz concerns semantic security.

1. You have designed a hardware decryption device $D$ that (unfortunately) emits a weak RF signal when decrypting. The client is worried that this signal could be used by a hacker to analyze the emitted signals, and get some side information.

You claim that the RF signals are random noise and independent of the decryption process. You would like to prove this using an argument similar to the one we used in class for semantic security.

That argument involved information about the plaintext $m$ captured by a function $f$. The case that no useful information would leak, was supported by stating that:

“For any adversary $\mathcal{A}$ and any polynomial-time computable function $f$ such that $\mathcal{A}$ can compute $f(m)$ given the ciphertext $c$ ($\Pr[\mathcal{A}(1^n, \text{Enc}_k(m)) = f(m)] = 1$), there is an adversary $\mathcal{A}'$ who is only given the length of the message $m$ (not $c$) that can compute $f(m)$ equally well (with negligible difference) ($\Pr[\mathcal{A}(1^n) = f(m)] = 1 - \varepsilon$)”

Modify this argument so that it addresses the security of your invention $D$ (of course, this will only address your client’s concern regarding information leakage).

Mike Burmester