a
if (tex.outputmode or tex.pdfoutput or 0) ¿ 0 then tex.print('““pdftrue') end

CS 466: Homework 3

Problem 1. (50 points.) Define key-generation algorithm $\mathcal{K}$ to output a random 128-bit key K and define encryption algorithm $\mathcal{E}$ by

```
Algorithm $\mathcal{E}_K(M)$:
    $C[0] \leftarrow\!\!\$\ \{0,1\}^{128}$
    For $i = 1$ to $m$ do:
        $W[i] \leftarrow C[0] + i \bmod 2^{128}$
        $C[i] \leftarrow \mathsf{AES}_K(M[i] \oplus W[i])$
    $C \leftarrow C[0] \| \ldots \| C[m]$
    Return $C$
```

Above we parse M as consisting of m blocks of 128-bits each, and '$W[i] \leftarrow C[0] + i \bmod 2^{128}$' denotes regarding $C[0]$ and i as encoding 128-bit integers, taking their sum modulo 2^{128}, and then encoding the result as another 128-bit string $W[i]$.

(Part A - 10 points.) Define a decryption algorithm $\mathcal{D}$ such that $\mathsf{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is a symmetric-key encryption scheme (i.e., satisfying the correctness condition we gave in class). You must use the definition of correctness given in class (which we wrote a couple equivalent ways). Half credit for an answer for an answer that has the right idea but is syntactically incorrect.

(Part B - 40 points.) Show that SE is not IND-CPA secure by giving a practical adversary A such that its advantage $\mathbf{Adv}^{\text{ind-cpa}}_{\mathsf{SE}}(A)$ is high. As usual, your adversary should be given in concise pseudocode and you should formally analyze its advantage and resource usage. NB: Your adversary should break the encryption scheme without breaking the underlying blockcipher as a PRF (no birthday attack or key recovery). Such attacks against the underlying blockcipher are not practical and will not receive any points. For full credit, make at most three queries and get advantage at least $c \cdot (1 - 2^{-128})$ for $c \geq 1/6$. Otherwise half credit.

Problem 2. (20 points.) There is a heated debate these days about encryption "backdoors." A backdoor is a means for accessing encrypted data if warranted by law enforcement. Check out the following links and give your own opinion. There is no right or wrong answer, I will give full credit to anyone who gives an informed opinion, and doesn't say anything factually untrue! Be concise and to the point: don't write more than 4 sentences.

Google "When encryption blocks justice" and go to the NYTimes Op-ed
`https://medium.com/@sweis/when-curtains-block-justice-142cbd0f3f34`
`https://www.wired.com/story/rod-rosenstein-encryption-backdoor/`
`https://www.wired.com/story/crypto-war-clear-encryption/`

https://blog.cryptographyengineering.com/category/backdoors/
https://www.schneier.com/academic/paperfiles/paper-keys-under-doormats-CSAIL.pdf