MTAT.07.003 Cryptology II
Spring 2012 / Exercise session ?? / Example Solution

Exercise (Insecurity of ECB mode of operation). *A block cipher is commonly modelled as a (t, q, ε)-pseudorandom permutation family $\mathcal{F}$. As such, it is perfect for encrypting a single block. The electronic codebook mode $\textsc{Ecb}_f(m_1, \ldots, m_n) = (f(m_1), \ldots, f(m_n))$ uses a same permutation $f \leftarrow \mathcal{F}$ for all message blocks. The latter is known to be insecure. Find an algorithm that can distinguish $\textsc{Ecb}_f : \mathcal{M}^n \to \mathcal{M}^n$ from a random permutation over $\mathcal{M}^n$. Is this weakness relevant in practise or not?*

Solution. Let us first formalise the the indistinguishability of $\textsc{Ecb}_f$ form a random permutation in terms of two games. In the first game $\mathcal{Q}_0$, the adversary $\mathcal{A}$ has an oracle access to the $\textsc{Ecb}_f(\cdot)$ function. In the second game $\mathcal{Q}_1$, the adversary $\mathcal{A}$ has an oracle access to a random permutation $f : \mathcal{M}^n \to \mathcal{M}^n$. Corresponding games where $\mathcal{F}_{\mathrm{perm}}$ denotes the set of all permutations over $\mathcal{M}^n$ are depicted below:

```
$\mathcal{Q}_0^{\mathcal{A}}$
    $f \leftarrow \mathcal{F}$
    return $\mathcal{A}^{\textsc{Ecb}_f(\cdot)}$
```

```
$\mathcal{Q}_1^{\mathcal{A}}$
    $F \leftarrow \mathcal{F}_{\mathrm{perm}}$
    return $\mathcal{A}^{F(\cdot)}$
```

The $\textsc{Ecb}_f$ is a (t, q, ε)-secure pseudorandom permutation if for all t-time adversaries who make at most q function calls the distinguishing advantage is bounded:

$$\mathsf{Adv}^{\mathrm{ind}}_{\mathcal{Q}_0,\mathcal{Q}_1}(\mathcal{A}) = \left|\Pr\left[\mathcal{Q}_0^{\mathcal{A}} = 1\right] - \Pr\left[\mathcal{Q}_1^{\mathcal{A}} = 1\right]\right| \leq \varepsilon \enspace .$$

To show the insecurity of $\textsc{Ecb}$ mode of operation it is sufficient to contract an efficient adversary that has large distinguishing advantage. For that, let us define an adversary $\mathcal{A}$ that makes a single oracle call for querying a message $\boldsymbol{m} = (m, m \ldots, m)$ and then outputs one if all blocks are the same:

```
$\mathcal{A}^{\mathcal{O}(\cdot)}$
    $(c_1, \ldots, c_n) \leftarrow \mathcal{O}(m, \ldots, m)$
    if $\exists i, j : c_i \neq c_j$ then return $0$
    else return $1$
```

If we substitute this definition into the games $\mathcal{Q}_0$ and $\mathcal{Q}_1$ we get simplified games:

```
$\mathcal{G}_0$
    $f \leftarrow \mathcal{F}$
    $c_1 \leftarrow f(m)$
    $\ldots$
    $c_n \leftarrow f(m)$
    if $\exists i, j : c_i \neq c_j$ then return $0$
    else return $1$
```

```
$\mathcal{G}_1$
    $F \leftarrow \mathcal{F}_{\mathrm{perm}}$
    $c_1 \xleftarrow{u} \mathcal{M}$
    $\ldots$
    $c_n \xleftarrow{u} \mathcal{M}$
    if $\exists i, j : c_i \neq c_j$ then return $0$
    else return $1$ .
```

Note that we can replace the evaluation of $F(\boldsymbol{m})$ in the game $\mathcal{G}_1$ by random sampling of output components, since the random permutation evaluated on a single argument gives a random element form $\mathcal{M}^n$ as a reply. In the game $\mathcal{Q}_0$, a fixed permutation f is evaluated on the same argument m and consequently $c_1 = \ldots = c_n$. As a result, we get

$$\Pr\left[\mathcal{G}_0 = 1\right] = 1 \qquad \text{and} \qquad \Pr\left[\mathcal{G}_1 = 1\right] = \frac{1}{|\mathcal{M}|^{n-1}} \enspace ,$$

from which we can conclude

$$\mathsf{Adv}^{\mathrm{ind}}_{\mathcal{Q}_0,\mathcal{Q}_1}(\mathcal{A}) = 1 - \frac{1}{|\mathcal{M}|^{n-1}} = \frac{|\mathcal{M}|^{n-1} - 1}{|\mathcal{M}|^{n-1}} \approx 1 \quad \text{for} \quad n > 1 \wedge |\mathcal{M}| > 1 \enspace .$$

Since $\mathcal{A}$ is very efficient algorithm, we can conclude that ECB mode of operation is not a (t, q, ε)-pseudorandom permutation for all practically relevant parameter values.

The scheme is vulnerable against practical attacks because the ciphertext leaks which plaintext blocks are identical. The effect is particularly pronounced when we encrypt images.

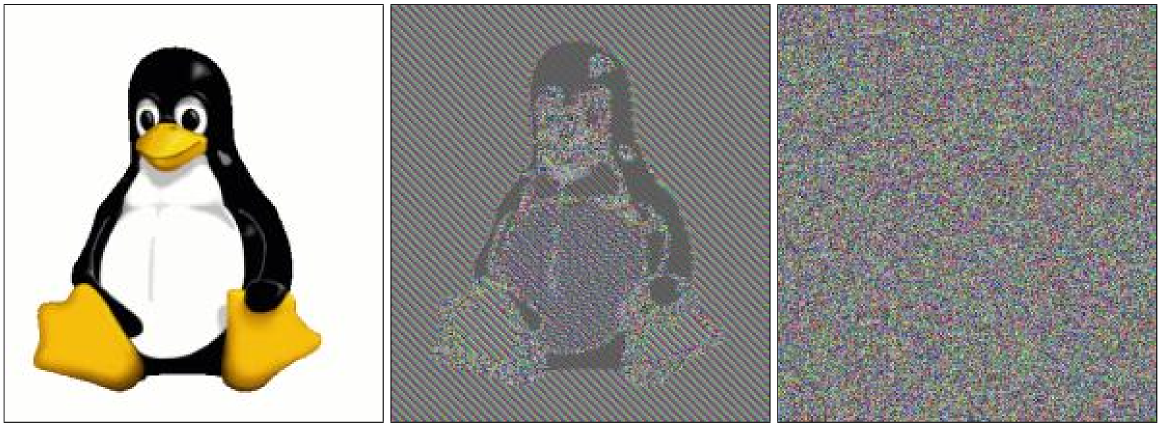

Figure 1: ECB mode of operation applied to an image file. Left pane is the original plaintext. The center pane is encrypted with the ECB mode of operation. The right pane is encrypted with secure pseudorandom permutation defined on the entire image. Pictures are courtesy of Wikipedia