**UConn, CSE Dept.**
**Fall 2024**
**CSE 3400/CSE 5850: Introduction to Computer and Network Security**
**/ Introduction to Cybersecurity**

# Practice Problems—Encryption

Instructor: Prof. Ghada Almashaqbeh

## Encryption

1. Let $f : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$ be an invertible PRP. For the following encryption construction, state whether it is secure against a CPA attacker. Given a message $m \in \{0,1\}^{2n}$ and key $k \xleftarrow{\$} \{0,1\}^{3n}$, define encryption as $E_k(m) = f_{k_1}(r) \parallel f_{k_2}(m_L) \parallel f_{k_3}(m_R)$, where $r$ is a random string of length $n$ generated fresh for each encryption, $k = k_1 \parallel k_2 \parallel k_3$, and $m = m_L \parallel m_R$.

   **Solution**
   Although this scheme might looks randomized, in the sense that a random $r$ is generated at random for each encryption and the PRP is invoked over that randomness, this scheme is still deterministic when it comes to the parts in the ciphertext about the message. That is, if you encrypt two messages $m$ and $m'$ such that $m = m'$, then the second and third parts of the ciphertext will be identical. So the CPA attacker will be able to guess the value of $b$ correctly. Thus, this cannot be CPA secure and the attacker advantage in wining the IND-CPA game is non-negligible.

2. Let $F : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a PRF. For the following encryption construction, state whether it is secure against a CTO attacker and whether it is secure against a CPA attacker. Given a message $m \in \{0,1\}^n$, define $E_k(m) = c = F_k(r) \oplus m$ with random $r \in \{0,1\}^n$ and the final ciphertext will be $(c, r)$.

   **Solution**
   Let's start with CPA attacker. $c$ is a pseudo-random string (the XOR of a pseudo-random string, which is the output of the PRF) with $m$ will produce a pseudo-random string) which does not tell anything about $m$. Same for $r$, it is a random string that is not related to $m$. The scheme is randomized since for each encryption invocation a new $r$ will be generated. So the attacker cannot tell (with non-negligible probability) which message $m_0$ or $m_1$ was encrypted in the IND-CPA game.

   The only event that may allow the attacker to distinguish and win the game is if any of the random strings $r$ has been reused again by the encryption oracle when encrypting the challenge ciphertext. But since $r$ is long enough and generated at random, and that we have an efficient attacker who can ask a polynomial number of encryption queries to the oracle, the probability this happen is negligible. So the scheme is secure against a CPA attacker.

Since the scheme is secure against the stronger CPA attacker, it is secure against the weaker CTO attacker.

In more formal terms, the proof of security will be a proof by reduction where we show that if the encryption scheme is insecure then we can build an attacker that breaks the PRF with non-negligible probability. So this is a contradiction, and hence, the encryption scheme is secure.

3. Let $P : \{0,1\}^n \times \{0,1\}^{2n} \rightarrow \{0,1\}^{2n}$ be an invertible PRP (i.e. a secure block cipher). Form an encryption as $E_k(m) = (r, P_k(r \parallel m))$, where $r$ is a random $n$ bit string generated fresh for each encryption invocation.

   What is the decryption algorithm? Is this an IND-CPA secure encryption scheme? Justify your answer.

   **Solution:** Decryption algorithm: let $c = P_k(r \parallel m)$, we have $r||m = D_k(r, c) = P^{-1}(c)$ $m$ is the last n bits of the output.
   This is an IND-CPA secure encryption scheme because it is a randomized secure block cipher. Since the evaluation of $P$ includes $r$, even if you encrypt the same message again, the ciphertext will be different and it picked at random from the output space (secure PRP is indistinguishable from a true random permutation, so the output does not carry any information about the input). As such, the attackers advantage is negligible.

   In more formal terms, the proof of security will be a proof by reduction where we show that if the encryption scheme is insecure then we can build an attacker that breaks the PRP security with non-negligible probability. So this is a contradiction, and hence, the encryption scheme is secure.