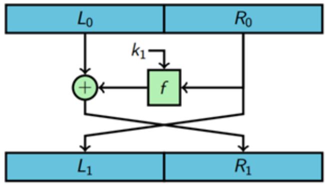
Final exam *Introduction to Cryptography VO*

Lecturer: Georg Fuchsbauer — 2 February 2021

1) (5+1 points)



a) A developer suggests making DES more efficient by running only **one** round of it, that is, one round of a Feistel network (as recalled in the figure). Explain why this does not even satisfy *indistinguishability in the presence of an eavesdropper* by **specifying an adversary**.

b) Does AES also use a Feistel network?

2) (1+2+3+3 points)

a) Let p be a positive polynomial. Is the function $f(n) := p(n) \cdot 2^{-\log n}$ negligible?

b) Is $(\{0,1\}^2, \oplus)$ a group? (That is, bitstrings of length 2 with bitwise XOR.) If not, why not? If yes, is it a cyclic group?

c) Does every provably secure (but not necessarily practical) encryption scheme have to assume the hardness of a computational problem? **Justify** your answer.

d) Consider an encryption scheme with message space $\{0,1\}^n$ and ciphertext space $\{0,1\}^\ell$. Why must we have $\ell \geq n$?

3) (3+3 points)

a) An engineer proposes the following symmetric encryption scheme for short messages, based on a pseudorandom function $F\colon \{0,1\}^n \times \{0,1\}^\ell \to \{0,1\}^\ell$: To encrypt a message $m \in \{0,1\}^\ell$ using key $k \in \{0,1\}^n$, choose $r \leftarrow \{0,1\}^\ell$ and return the ciphertext $c := F_k(r) \oplus m$. Would you recommend using the scheme if CCA-security is *not* required? **Justify** your answer.

b) An engineer suggests a new hash function $H\colon \{0,1\}^* \to \{0,1\}^{80}$ and claims to have proved its collision-resistance. Why would you **not** use it?

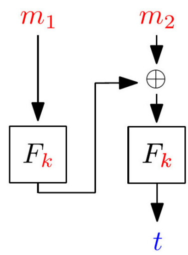
4) (4+4 points)

Let p and q be two equal-length primes; define $N := p \cdot q$ and let e be such that $\gcd(e, \phi(N)) = 1$. The RSA function is defined as: $f_{(N,e)}(x) := [x^e \bmod N]$.

a) What is the RSA **assumption**?

b) How can you invert $f_{(N,e)}$ **efficiently** if you know the factorization of N?

5) (5+5 points)



a) Let $F : \{0,1\}^n \times \{0,1\}^\ell \to \{0,1\}^\ell$ be a blockcipher. Show that "basic CBC-MAC" (as recalled in the figure) constructed from F is **not secure**(*) when messages from $\{0,1\}^\ell$ (in which case $\mathsf{Mac}_k(m) := F_k(m)$) **and** from $\{0,1\}^{2\cdot\ell}$ are allowed.

b) Why is the authenticated-encryption method "*encrypt and authenticate*", defined as: $\mathsf{Enc}'_{(k_E,k_M)}(m) := \mathsf{Enc}_{k_E}(m) \,\|\, \mathsf{Mac}_{k_M}(m)$ not CPA-secure when basic CBC-MAC is used as the MAC scheme? **Show an attack.**

6) (3+6+2 points)

Consider the following deterministic variant of Schnorr signatures using a standardized group $(\mathbb{G}, q, g)$ and a standardized hash function $H\colon \{0,1\}^* \to \mathbb{Z}_q$.

- Gen:
  - choose $x \leftarrow \mathbb{Z}_q$ and $k \leftarrow \mathbb{Z}_q$
  - return $pk = (h = g^x)$ and $sk = (pk, x, k)$
- $\mathsf{Sign}_{sk}(m)$:
  - compute $I := g^k$
  - compute $r := H(I, m)$
  - compute $s := [r \cdot x + k \bmod q]$
  - return (r, s)
- $\mathsf{Vrfy}_{pk}(m, (r, s))$:
  - compute $I := g^s \cdot h^{-r}$
  - return 1 iff $H(I, m) = r$

a) Show that this scheme is **correct**.

b) Is this scheme **secure**(*) (when modeling the hash function as a random function)? Justify your answer.

c) Explain at least two advantages of digital signatures over message authentication codes.

(*) in the standard sense of *existential unforgeability under adaptive chosen-message attacks*