Applied Cryptography

thghoebel@ethz.ch

ETH Zürich, FS 2021

This documents is a **short** summary for the course *Applied Cryptography* at ETH Zurich. It is intended as a document for quick lookup, e.g. during revision, and as such does not replace reading the slides or a proper book.

We do not guarantee correctness or completeness, nor is this document endorsed by the lecturers. Feel free to point out any erratas.

Contents

1 Symmetric Cryptography

One-time pad Plaintext p, key k such that $|p| = |k|$. Ciphertext $c = p \oplus k$.

If k u.a.r. and only used once then the OTP is **perfectly secure**, i.e. $\Pr[P = p|C = c] = \Pr[P = p]$.

Note: keys can re-occur (as a result of random sampling) but they must not be re-used (i.e. the adversary must not be aware that the same key is used).

Issues: same lengths, key distribution, single use.

1.1 Block Ciphers

Block cipher A block cipher with key length k and block size n consists of two efficiently computable permutations[1]:

$$E : \{0,1\}^k \times \{0,1\}^n \mapsto \{0,1\}^n \quad D : \{0,1\}^k \times \{0,1\}^n \mapsto \{0,1\}^n$$

such that for all keys K D_K is the inverse of E_K (where we write E_K short for $E(K, \cdot)$).

Security notions Known plaintext attack, chosen plaintext attack, chosen ciphertext attack. Exhaustive key search on (P, C) pairs – no attack should be better, else we throw the cipher away.

Pseudo-randomness

- Adversary $\mathcal{A}$ interacts either with block cipher (E_K, D_K) or a truly random permutation (Π, Π^{-1}).
- A block cipher is called a **pseudo-random permutation PRP** if no efficient[2] $\mathcal{A}$ can tell the difference between E_K and Π (no access to the inverse).
- A block cipher is called a **strong-PRP** if no efficient $\mathcal{A}$ can tell the difference between (E_K, D_K) and (Π, Π^{-1}).

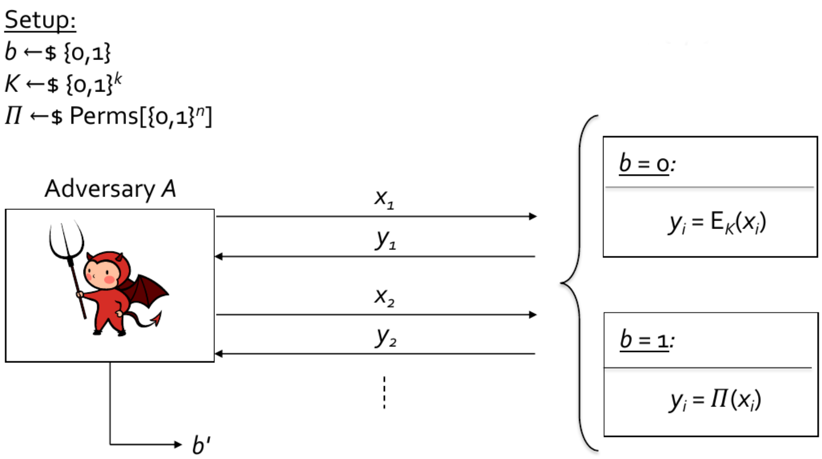

Figure 1: PRP game pictorially

[1] Encipher and decipher
[2] Quantified by runtime + number of oracle queries.

The advantage is defined as:

$$\mathbf{Adv}_E^{PRP}(\mathcal{A}) = 2 \cdot \left| \Pr[\text{Game}\mathbf{PRP}(\mathcal{A}, E) \Rightarrow \text{true}] - \frac{1}{2} \right|$$

where the probability is over the randomness of $b, K, \Pi, \mathcal{A}$.

Constructing block ciphers In general: keyed round function that is repeated many times.

- Feistel cipher: halved blocks crossing back and forth, e.g. DES
- Substitution-permutation network: confusion + diffusion, e.g. AES

1.2 Symmetric Encryption

1.3 Hash Functions

1.4 Message Authentication Codes MACs

1.5 Authenticated Encryption