Introduction to cryptology
TD#2

2024–W7

Exercise 1: PRF attacks

Q.1: We consider an arbitrary function $\mathsf{F} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$.

1. Show that:
$$\mathbf{Adv}_{\mathsf{F}}^{\mathrm{PRF}}(2, 2^n) \approx 1$$

⋆. Show that:
$$\mathbf{Adv}_{\mathsf{F}}^{\mathrm{PRF}}(1, 2^n) \approx 1$$

3. What minimal value would you advise for n, if your objective is that F should resist a planetwise PRF attack?
4. Is taking n as previously sufficient to guarantee that F is a "good" PRF?

Q.2: We now assume that F is such that there is a subset $\mathcal{S}$ of its keys with the property that for all $k \in \mathcal{S}$, $\mathsf{F}(k, 0) = 0$ (i.e. 0 is a *fixed-point*). We let 2^w denote the size of $\mathcal{S}$, for some $w \in [\![0, n]\!]$.

1. Propose a PRF attack on F exploiting the above property that makes one query to its oracle and runs in time one; give a lower-bound of its advantage.
2. Informally prove or disprove the following informal statement: "It is hard to predict the output of a good PRF".

Exercise 2: CTR mode with random counters

For the sake of simplicity and without loss of generality, we only consider a mode of operation for n-bit messages.

Let F be as in the previous exercise. We define CTR\$[F], the CTR mode with random counters instantiated with F in the following way:

— Setup: draw $k \twoheadleftarrow \{0,1\}^n$

— Every time a message m needs to be encrypted:

1. Draw $r \twoheadleftarrow \{0,1\}^n$
2. Send $(r, \mathsf{F}(k, r) \oplus m)$

Q.1

1. Show that an adversary able to observe two ciphertexts with the same value r is able to deduce information about the plaintexts.
2. Give an upper-bound for the probability that this happens, in function of the number q of messages that have been encrypted.
3. Would you say that CTR\$ is "secure beyond the birthday bound"?
4. How does the security of CTR\$ compare with the one of the "usual" CTR mode if F is a "good" PRP with n bits of security (meaning here that it takes time $\propto 2^n$ to distinguish it from a uniform permutation with constant advantage)? And if it is a "good" PRF (with the same meaning)?

Exercise 3: A game of martens and squirrels *(Adapted from final exam '21)*

The cute and clever pine marten (*martes martes*) is out in the woods hunting for the dim and pouchy grey squirrel (*sciurus carolinensis*). From a previous scouting mission, the marten knows that the squirrel sleeps every night in a different place, and it has carefully mapped all N such places. It also knows that the squirrel divides its time in N-day cycles and only sleeps once at every place per such cycle. The squirrel, aware of the presence of the marten, tries to always change the order in which it visits its sleeping grounds from one cycle to the other.

Q.1: The marten can visit T places per night to try catching the squirrel. Specify a simple hunting strategy for the marten that guarantees that it will catch the squirrel in at most $\mathsf{N} - \mathsf{T}$ nights.

Q.2: The marten being quite slender, it cannot reasonably expect to survive for $\mathsf{N} - \mathsf{T}$ nights (for typical values of N and T) without catching a squirrel. It is however highly skilled in scouting and astronomy, and so is always able to determine where the squirrel slept the *one* previous night and what is the day position in the current cycle (from 1 to N). Additionally, the squirrel —being quite silly— only uses a very primitive way of determining its sleeping schedule: at the start of every cycle, it picks $k \twoheadleftarrow [\![0, \mathsf{N} - 1]\!]$ uniformly at random, and then decides that it will spend the i^{th} night of the cycle at place $i + k \mod \mathsf{N}$ (where $a \mod b$ denotes here the unique non-negative remainder $\in [\![0, b - 1]\!]$ of the division of a by b), for some fixed numbering of the sleeping places (i.e. one that does not change from one cycle to another).

1. Assuming that the marten already knows the numbering of sleeping places used by the squirrel, give a strategy that guarantees that it will catch the squirrel within at most two nights.
2. Show that the former assumption is not necessary if the marten can spend one full cycle observing the squirrel (for instance because it found alternative food, see Figure 1).

Q.3:

1. Show that the squirrel's strategy may be understood as implicitly using a block cipher, and give a general formulation thereof using an abstract "format-preserving" block cipher $\mathsf{E} : \mathcal{K} \times [\![0, \mathsf{N} - 1]\!] \to [\![0, \mathsf{N} - 1]\!]$.
2. Show informally that for this strategy, the marten's chance of quickly catching the squirrel is essentially related to the UP insecurity of the squirrel's chosen block cipher.

Figure 1: A coping strategy. Photo: Vince Smith.