Private Key Encryption

Computational security

1.Security is only guaranteed against efficient adversaries that run for some feasible amount of time

2. Adversaries can potentially succeed (i.e., security can potentially fail) with some very small probability.

Computational secrecy?

- Idea: relax perfect indistinguishability

- Two approaches
  - Concrete security
  - Asymptotic security

Computational indistinguishability (concrete)

A scheme is (t, ε)-secure *if any adversary running for time at most* t *succeeds in breaking the scheme with probability at most* ε.

- (t, ε)-indistinguishability:
  - Security may fail with probability ≤ ε
  - Restrict attention to attackers running in time ≤ t
    - Or, t CPU cycles

Asymptotic security

- Introduce *security parameter* n
  - For now, think of n as the key length

A scheme is secure if any ppt adversary succeeds in breaking the scheme with at most negligible probability.

Ppt-probabilistic polynomial-time

Efficient algorithms

A function f from the natural numbers to the nonnegative real numbers is polynomially bounded

- if there is a constant c such that $f(n) < nc$ for all n.
- An algorithm A runs in polynomial time if there exists a polynomial p such that, for every input $x \in \{0,1\}*$, the computation of $A(x)$ terminates within at most $p(|x|)$ steps

Negligible success probability.

- A negligible function is one that is asymptotically smaller than any inverse polynomial function. Formally:
- *A function f from the natural numbers to the nonnegative real numbers is negligible if for every polynomial **p** there is an **N** such that for all n > N it holds that .*

$$f(n) < \frac{1}{p(n)}$$

Negligible functions

Let $negl_1$ and $negl_2$ be negligible functions. Then,

- 1. The function

  $negl_3(n) = negl_1(n) + negl_2(n)$ is negligible.

- 2. For any polynomial p, the function

  $negl_4(n) = p(n) \cdot negl_1(n)$ is negligible.

Asymptotic Security

A scheme is **secure** if for *every probabilistic polynomial-time* adversary A carrying out an attack, the probability that A succeeds in the attack is *negligible*.