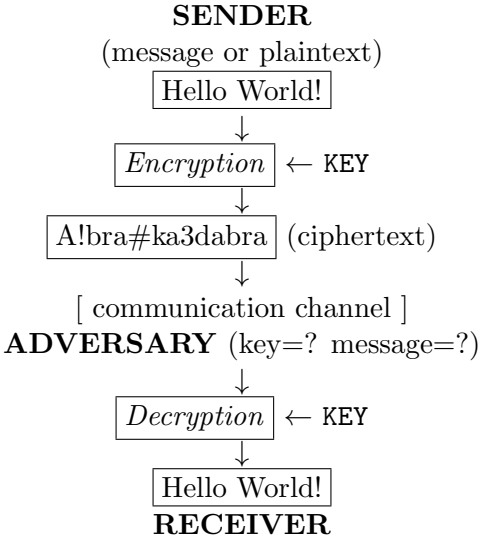
MMA Advanced Lecture I: Introduction and Motivation

Instructor: Kirill Morozov (IMI)
Scribe: Shun'ichi Yokoyama (Kyushu university)

April 15th, 2011

This course's subtitle is **"Randomness Extraction and its Applications to Cryptography"**. "Cryptography" comes from Greek "kryptos" (hidden, secret) and "gráphin" (writing). Similarly, in Japanese "暗号" (dark - number).



Kerckhoff's principle: All the information about an encryption scheme, except for the (secret) key must be publicly known.

In other words, only secrecy of the key makes an encryption secure.

Cryptography

Before 1970
Art of encryption
= secure data exchange over insecure channels
↓
After 1970
Science of communication and computation with privacy

List of important cryptographic applications: (short and incomplete)

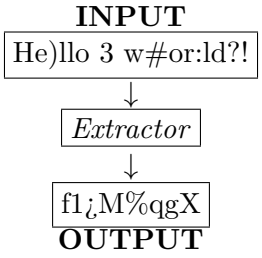
- **Digital signature:** to ensure safety of software and web-applications.
- **Authentication schemes:** online services, physical access (buildings, cars, etc.).
- **Secure multi-party computation:** electronic voting, protection of medical data, e-auctions etc.

etc.

In short, cryptography provides us with privacy and safety. And randomness is very important in cryptography.

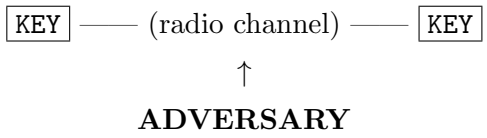
Cryptography as secure as the secret information (key, password, etc.) which must be random (or hard to guess: uniform in the ideal case) from the adversary's point of view.

What if the distribution of the shared secret is not uniform?? — Then, an **extractor** can be used to obtain an (almost) uniform output an input which has enough randomness.



Applications of randomness extraction to cryptography:

- **Pseudorandom generators from any one-way function:** (Fundamental theoretical result) How to use cryptography to generate "random-like" sequences.
- **Biometrics:** Biometric data are not purely random, but "noisy". This randomness can be extracted for cryptographic purposes: authentication etc.
  Example: Iris patterns of an eye.
- **Unbreakable (information-theoretically secure) keys from random noise:**



(Even with the strongest supercomputer (adversary) cannot learn the `KEY` !!)

- **Leakage-resilient cryptography:** Standard cryptographic schemes provide security guarantees only if the key assumed completely unknown to adversary. What if some part of the key (say, one half of it) has leaked to the adversary?
  Leakage-resilient cryptography studies schemes, which are secure even in case of the key leakage. Exposure-resilient functions and all-or-nothing transforms are used, in particular, in this setting.

PLAN OF THIS COURSE

1. **Background**

   - Elements of probability theory and information theory
   - Pairwise independence and universal hashing
   - Leftover Hash Lemma (LHL): with proof and some variants
     # On the way, we will discuss some basic cryptographic schemes and techniques.

2. **Applications** (if time permits)

   - Information-theoretic key agreement from random noise: setting, security definition, protocol(s)
   - Pseudorandom generators from any one-way permutation: related security definitions, construction, proof sketch
   - Expose-resilient functions: security definitions, one construction, relation to all-or-nothing transforms

Note: Cryptography interacts with different areas of mathematics:

Information theory, **Probability theory**,
Linear algebra, Number theory, Graph theory, Combinatorics,
Algorithm theory, Complexity theory, Coding theory, ...

Of course, cryptography uses results and techniques from these areas, but also it contributes new results. For instance, randomness extractors were first (implicitly) used in the cryptographic construction of pseudorandom generators. Nowadays, extractors are used in complexity theory, randomized algorithms and error-correcting codes, to name a few.

$***$

※ **The rest of the presentation followed the textbook, pages 207-208, up to and including Example 8.3.**