1 About Assignments and About Test

- Assignments 1-7 by Saturday $\Rightarrow$ Extra Vernam
- Assignments 1-8 by Tuesday $\Rightarrow$ Extra Hill

Practice test posted on eClass, and the test is on February 1 (Only on Probability Theory, and nothing on Ciphersystems)

2 Kerchov's Principles

1883 Auguste Kerchov in *La Cryptographie Militaire*, six design principles for military ciphers.

1. The system must be practically, if not mathematically, indecipherable.
2. It must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience.
3. Its key must be communicable and retainable without the help of written notes, and changeable or modifiable at the will of the correspondents.
4. It must be applicable to telegraphic correspondence
5. It must be portable, and its usage and function must not require the concourse of several people.
6. Finally, it is necessary, given the circumstances that command its application, that the system be easy to use, requiring neither mental strain nor the knowledge of a long series of rules to observe.

3 Probability Vocabulary

Definition 1 (Experiment, Random Variables)**.** This refers to an activity, not necessarily scientific, which involves the production of data some of which are "random". We denote an experiment by $\mathcal{E}$ and the data by $X, Y, Z, \ldots$. The latter are usually referred to as the *random Variables*, associated with $\mathcal{E}$.

Definition 2 (Random, Sample Space, Probabilities)**.** We use the word *random* whenever $X, Y, Z, \ldots$ we are studying are produced by such an intricate mechanism that all we know about them is

1. The range of possible values that $X, Y, Z, \ldots$ may take. This range is usually referred to as the *sample space* and is denoted by Ω.
2. Certain positive numbers are called *probabilities* which numerically express our "confidence" that $X, Y, Z, \ldots$ fall in chosen subsets of the sample space Ω.

Definition 3 (Elementary Outcome, Sample Point)**.** An individual outcome of the experiment $\mathcal{E}$ is usually referred to as an *elementary outcome* or *sample point*. Mathematically this is just an element of the sample space Ω.

Definition 4 (Event)**.** Mathematically an *event* is just a subset of Ω. We say that $\mathcal{E}$ "resulted in the event A" or that "A has occurred" if the outcome falls in the subset A.

Definition 5 (Field of Events)**.** The collection of events associated with our experiment $\mathcal{E}$ is usually denoted by $\mathcal{F}$. In other words, $\mathcal{F}$ denotes the collection of subsets of the sample space Ω that are of special interest in our study. For mathematical reasons, $\mathcal{F}$ is assumed to be closed under the set operations of intersection, union, and complementation. Two subsets $\emptyset$ and Ω are always included in $\mathcal{F}$.

Definition 6 (Probability Measure)**.** Our experiment $\mathcal{E}$ associates to each event A of $\mathcal{F}$ a number $P(A)$ in the interval $[0, 1]$ which reflects our confidence that the outcome falls in A. We refer to $P(A)$ as the probability of A. Note that we should have $P(\Omega) = 1$ and that if A and B are mutually exclusive events, then

$$P(A \cup B) = P(A) + P(B)$$

A set function with these properties is usually referred to as a *probability measure*.

Definition 7 (Expectation of a Random Variable)**.** Any function of the measure of our experiment can be referred to as a *random variable*. Mathematically, a random variable is simply a function of the sample space. If the events $A_1, A_2, ..., A_n$ are mutually exclusive and decompose Ω, and the random variable X takes the value x_i when A_i occurs, then the expression

$$\mathbb{E}[X] = \sum_{i=1}^{n} x_i P(A_i)$$

is referred to as the *expectation of* X. If we repeat $\mathcal{E}$ a very large number of times, and average out the successive values of X we get, then we should expect the resulting average to be close to $\mathbb{E}[X]$.

Definition 8 (Conditional Probability)**.** If A and B are events and the ratio

$$P(A \mid B) = \frac{P(A \cap B)}{P(B)}$$

is usually referred to as the *conditional probability of A given B*. The concept arises as follows. Given the event B we can construct a new experiment $\mathcal{E}_B$ by carrying out $\mathcal{E}$ and recording its outcome only when it falls in B. We can argue that the probability of A under $\mathcal{E}_B$ will is $P(A \mid B)$ where $P(A \cap B)$ and $P(B)$ are the probabilities of $A \cap B$ and B under $\mathcal{E}$. We shall refer to $\mathcal{E}_B$ as $\mathcal{E}$ crippled by B.

Definition 9 (Conditional Expectation of a Random Variable)**.** Given an event B, if we carry out the crippled experiment $\mathcal{E}_B$ instead of $\mathcal{E}$, then all the probabilities change and so do all expectations. If X is a random variable and the events $A_1, A_2, ..., A_n$ decompose Ω as before then

$$\mathbb{E}[X \mid B] = \sum_{i=1}^{n} x_i P(A_i \mid B)$$

gives the expected value of X under $\mathcal{E}_B$. We refer to it as the *conditional expectation of X given B*.

Definition 10 (Dependence)**.** The random variable Y is said to be *dependent* upon the random variable X if and only if Y is a function of X. Similarly, we say that Y is dependent upon $X_1, X_2, ..., X_n$ if for some $f(X_1, X_2, ..., X_n)$ we have

$$Y = f(X_1, X_2, ..., X_n)$$

Definition 11 (Independence)**.** In probability theory, "independence" is not the negation of "dependence". We say that Y is independent of X if and only if knowing the value of X does not change the uncertainty of Y. More precisely, if we cripple our experiment $\mathcal{E}$ by any events $X = a$, the probabilities of all events $Y = b$ do not change. Mathematically this is translated in the conditions that for all choices a and b,

$$P(Y = b \mid X = a) = P(Y = b)$$

which also means that

$$P(Y = b \cap X = a) = P(X = a)P(Y = b)$$

4 Conditional Probability

5 Dependence and Independence