Introduction to cryptology
TD#1

2020-W06,W07

Exercise 1: The mysterious egg problem

There are many possible formulations for this classical exercise (some of them more bloody than others). We will adopt the following.

An explorer found a basket of mysterious eggs, and wants to determine up to what height (in metres) they can fall without breaking (we assume that an upper-bound n (e.g. 100m) is known; also, the eggs are magical and are not damaged by a fall that doesn't break them). Our explorer does not want to break too many eggs to find out the answer, but also wishes to avoid making too many trials (as each of them requires to climb up to a certain height, drop an egg, and climb or rappel down to the ground to find out if it is broken). You need to help him/her in determining the following tradeoffs.

Q.1: Describe an algorithm that breaks one egg and needs n drops in the worst case.

Q.2: Describe an algorithm that breaks up to $\lceil \log_2(n) \rceil$ eggs and needs $\mathcal{O}(\log_2(n))$ drops in the worst case.

Q.3: Describe an algorithm that breaks two eggs and needs $\mathcal{O}(\sqrt{n})$ drops in the worst case.

Note. The last algorithm is an instance of a "baby-step giant-step" method, that is also useful to compute discrete logarithms (i.e. logarithms in a finite group).

Exercise 2: One-time pad

Q.1: Let x, r be two independent random variables over $\mathbb{F}_2$[1], r being drawn uniformly at random (i.e. $\Pr[r = 0] = \Pr[r = 1] = 0.5$) and x being 0 with some probability p. What is:

— $\Pr[x + r = 0]$?

— $\Pr[x + r = 1]$?

— $\Pr[x = 0 | x + r = 0]$?

— $\Pr[x = 0 | x + r = 1]$?

— $\Pr[x = 1 | x + r = 0]$?

— $\Pr[x = 1 | x + r = 1]$?

Hint. You may use Bayes' formula: $\Pr[A|B] = \Pr[B|A] \Pr[A] / \Pr[B]$.

[1] In this question, $\mathbb{F}_2$ denotes the finite field with two elements, also sometimes written $\mathbb{Z}/2\mathbb{Z}$.

Q.1 bis: Recompute $\Pr[x = 0|x + r = 0]$ for an arbitrary $\Pr[r = 0] = q$. What comment can you make when comparing with the previous case?

Q.2: Let $\vec{x} \in \mathbb{F}_2^n$ and $\vec{r}$ be an element drawn uniformly at random from $\mathbb{F}_2^n$. For each element $\vec{y}$, $\vec{z}$ of $\mathbb{F}_2^n$, what is $\Pr[\vec{x} + \vec{r} = \vec{y}]$? $\Pr[\vec{x} = \vec{z}|\vec{x} + \vec{r} = \vec{y}]$?[2]

Q.3: Assume that $x \in \{0,1\}^n$ is a message written as binary data. Assume that $r \in \{0,1\}^n$ is drawn uniformly at random among all binary strings of length n. Explain why observing $x \oplus r$ (the bitwise XOR of x and r) does not reveal any information about x.

Q.4: We will say that a cipher $\mathcal{C}$ offers *perfect confidentiality* (which isn't really a formal notion, and is not sufficient for a full cryptosystem to be secure) if observing the *ciphertext* $c = \mathcal{C}(p)$ does not reveal any new information about the *plaintext* p.

Let p and k be n-bit strings. Under what condition on k is the cipher $\mathcal{C} : p \mapsto p \oplus k$ perfectly confidential?

Q.5: Let $\mathcal{C}$ be a perfectly confidential cipher as above. Is its concatenation $\mathcal{C}^2 : p||p' \mapsto p \oplus k||p' \oplus k$ perfectly confidential?

Exercise 3: (multi-)collisions

In this exercise, we let $\mathcal{S}$ be an arbitrary finite set of size N, and we denote by $X \xleftarrow{\$} \mathcal{S}$ the process of drawing X from $\mathcal{S}$ uniformly at random, and independently of any other process.

Let $X \xleftarrow{\$} \mathcal{S}$, $Y \xleftarrow{\$} \mathcal{S}$, $Z \xleftarrow{\$} \mathcal{S}$.

1. Compute $\Pr[(X = x) \wedge (Y = y)]$ for any $x, y \in \mathcal{S}$.
2. Compute $\Pr[X = Y]$.
3. Compute $\Pr[X = Y = Z]$.

Exercise 4 🌶: Finite groups, finite fields, $\mathbb{F}_2$, $\mathbb{F}_2^n$

A *commutative group* $(\mathbb{G}, \star)$ is defined by a non-empty set of elements $\mathbb{G}$ and an operation $\star$ that satisfies the following properties:

1. $\mathbb{G}$ is closed by $\star$: $\forall\, a, b \in \mathbb{G}$, $a \star b \in \mathbb{G}$
2. There is a neutral (or identity) element: $\exists\, e \in \mathbb{G}$ s.t. $\forall\, a \in \mathbb{G}$, $a \star e = a$
3. The law $\star$ is associative: $\forall\, a, b, c \in \mathbb{G}$, $a \star (b \star c) = (a \star b) \star c$
4. Every element of $\mathbb{G}$ is invertible: $\forall a \in \mathbb{G}$, $\exists\, b$ s.t. $a \star b = e$
5. The law $\star$ is commutative: $\forall\, a, b \in \mathbb{G}$, $a \star b = b \star a$

The size (or cardinality) of $\mathbb{G}$ (i.e. the number of elements it contains) is called the *order* of the group.

A group is usually written either additively ($\star$ is denoted $+$; the inverse of an element a is denoted $-a$; the neutral element is noted 0) or multiplicatively ($\star$ is denoted $\cdot$ or $\times$ or nothing; the inverse of an element a is denoted $1/a$ or a^{-1}; the neutral element is noted 1).

Common examples of groups are $(\mathbb{Z}, +)$ (the relative integers with addition), $(\mathbb{R}, +)$ (the real numbers with addition) or $(\mathbb{R}\backslash\{0\}, \times)$ (the real numbers except zero with multiplication). Note that $(\mathbb{N}, +)$ is not a group (only 0 has an inverse). It is possible for a group to only

[2] For simplicity, $\vec{x}$ etc. can be thought of as n-bit binary strings.

contain a finite number of elements; in that case we say that it is *discrete* or finite. Examples of finite groups of order n are the integers modulo n with addition, usually written $(\mathbb{Z}/n\mathbb{Z}, +)$.

A finite group is called *cyclic* if it is *generated* by a single element. So $\mathbb{G}$ (written multiplicatively) is cyclic iff. $\exists\, g \in \mathbb{G}$ s.t. $\forall\, h \in \mathbb{G}$, $\exists\, x \in \mathbb{N}$ s.t. $h = g^x$.

For any g in some group $\mathbb{G}$, we may write $\langle g \rangle$ for the group *generated* by this element, i.e. the group whose elements are $\{1 = g^0, g, g^2, \ldots\}$; this is a *subgroup* of $\mathbb{G}$. If g is in a finite group, then $\exists\, n \in \mathbb{N}$ s.t. $g^n = g^0 = 1$. The least such integer is called the *order* of g. In particular, this means that g is a generator of $\mathbb{G}$ (i.e. $\mathbb{G} = \langle g \rangle$) iff. the order of g is equal to the order of $\mathbb{G}$.

If $h \in \mathbb{G}$ and $\mathbb{G}' := \langle h \rangle \neq \mathbb{G}$, then we say that $\mathbb{G}'$ is a *proper subgroup* of $\mathbb{G}$. Furthermore, if $\mathbb{G}$ is finite of order N, then the order of $\mathbb{G}'$ must be a divisor of N.[3] A consequence of this is that if $\mathbb{G}$ is of prime order, its only proper subgroup is the trivial group $\{1\}$, and every other element is a generator.

Let $\mathbb{G} = \langle g \rangle$ be a finite group of order N. The *discrete logarithm* in base g (or *w.r.t.* g) of $h \in \mathbb{G}$ is the integer $x \in [\![0, N-1]\!]$ s.t. $g^x = h$.

Q.1: What is the order of $(\mathbb{Z}/7\mathbb{Z}, +)$ and $(\mathbb{Z}/7\mathbb{Z}\backslash\{0\}, \times)$? Why isn't $(\mathbb{Z}/9\mathbb{Z}\backslash\{0\}, \times)$ a group?

Q.2: What is the discrete logarithm of 5 in $(\mathbb{Z}/7\mathbb{Z}, +)$ in base 1?

Same question in $(\mathbb{Z}/7\mathbb{Z}\backslash\{0\}, \times)$ in base 3? Why wouldn't the same question make sense in base 1?

*

A *field* $(\mathbb{K}, +, \times)$ is defined by a set of elements $\mathbb{K}$ and two operations (here $+$ and $\times$) such that:

1. $(\mathbb{K}, +)$ is a commutative group.
2. $(\mathbb{K}\backslash\{0\}, \times)$ is a commutative group, where 0 is the neutral element of $(\mathbb{K}, +)$.
3. The element 0 is absorbing for $\times$, i.e. $\forall\, a \in \mathbb{K}$, $a \times 0 = 0$.
4. The law $\times$ is distributive over $+$: $\forall\, a, b, c \in \mathbb{K}$, $a \times (b + c) = a \times b + a \times c$.

Common examples of fields are $(\mathbb{R}, +, \times)$ (the real numbers with addition and multiplication) and $(\mathbb{Q}, +, \times)$ (the rational integers with addition and multiplication). A counter-example is $(\mathbb{Z}, +, \times)$, as only 1 and -1 have a multiplicative inverse, i.e. $(\mathbb{Z}\backslash\{0\}, \times)$ is not a group.

If in the above one considers a structure $(\mathbb{A}, +, \times)$ that satisfies 1, 3, 4 but only a weaker variant of 2 by asking that $(\mathbb{A}\backslash\{0\}, \times)$ is only a *monoid* (i.e. not all of its elements need to be invertible), then $\mathbb{A}$ is a *ring*. Since a group is a monoid, if $\mathbb{K}$ is a field then it is also a ring, but the converse is not true. In the above examples, $(\mathbb{Z}, +, \times)$ is a ring that is not a field.

For an arbitrary ring $\mathbb{A}$, it is usual to write $\mathbb{A}^\times$ for the *multiplicative group* of $\mathbb{A}$. When $\mathbb{A}$ is a field, this coincides with $(\mathbb{A}\backslash\{0\}, \times)$ but when it is not this denotes the subset of $\mathbb{A}$ in which all elements have an inverse for the multiplication. For instance, $\mathbb{Z}^\times = \{1, -1\}$.

It is not necessary for a field to have an infinite number of elements. Examples of *finite fields* are the integers modulo a prime number p, which have p elements. Such fields are usually written as $\mathbb{Z}/p\mathbb{Z}$ or $\mathbb{F}_p$.

Q.3: Which of the followings are fields: $(\mathbb{N}, +, \times)$, $(\mathbb{C}, +, \times)$, $(\mathbb{Z}/7\mathbb{Z}, +, \times)$, $(\mathbb{Z}/33\mathbb{Z}, +, \times)$?

[3] This is a theorem due to Lagrange.

Q.4: What are the elements of $(\mathbb{Z}/5\mathbb{Z})^\times$? What about $(\mathbb{Z}/6\mathbb{Z})^\times$?

Q.5: Give the addition and multiplication tables of the field $\mathbb{F}_2$ (denotinh its only two elements by 0 and 1). What happens when an element of the field is added to itself an even number of times? An odd number?

*

Let $\mathbb{K}$ be a field; a $\mathbb{K}$-vector-space E is a set of vectors endowed with an *inner addition law* ($+$, used to add vectors together) and an *outer multiplication law* ($\times$, used to multiply a vector by a scalar from $\mathbb{K}$). A vector-space must satisfy the following:

1. $(E, +)$ is a commutative group.
2. The multiplication law must be such that $\forall\, \vec{u}, \vec{v} \in E$, $\forall\, \lambda, \mu \in \mathbb{K}$:
   (a) $\lambda(\vec{u} + \vec{v}) = \lambda\vec{u} + \lambda\vec{v}$.
   (b) $(\lambda\mu)\vec{u} = \lambda(\mu\vec{u})$.
   (c) $(\lambda + \mu)\vec{u} = \lambda\vec{u} + \mu\vec{u}$.
   (d) $1\vec{u} = \vec{u}$.

Two vectors $\vec{u}$, $\vec{v}$ are *linearly independent* iff. $\nexists \lambda \in \mathbb{K}$ s.t. $\lambda\vec{u} + \vec{v} = \vec{0}$, where the *null vector* $\vec{0}$ is the neutral element for $(E, +)$. More generally, n vectors are linearly independent iff. there is no linear combination of any of them that sums to the null vector. The *dimension* $\dim(E)$ of a vector-space E is equal to the maximum size of a family of linearly independent vectors of E. Note that this dimension is not necessarily finite.

A *basis* of a finite-dimensional vector-space is a family of $n = \dim(E)$ linearly-independent vectors $\vec{b_0}, \ldots, \vec{b_{n-1}}$ such that all vectors of E can be written as a linear combination of elements of the basis: $\forall\, \vec{u} \in E$, $\exists\, \lambda_0, \ldots, \lambda_{n-1} \in \mathbb{K}$ s.t. $\vec{u} = \lambda_0\vec{b_0} + \ldots + \lambda_{n-1}\vec{b_{n-1}}$.

An example of vector-space of dimension 2 is $\mathbb{R}^2$. Two possible bases for this vector-space are $\begin{pmatrix}1 & 0\end{pmatrix}^t$, $\begin{pmatrix}0 & 1\end{pmatrix}^t$ and $\begin{pmatrix}1 & 2\end{pmatrix}^t$, $\begin{pmatrix}1 & 1\end{pmatrix}^t$. An example of vector-space of infinite dimension is $\mathbb{R}[X]$, the polynomials with coefficients in $\mathbb{R}$. A possible (infinite) basis for this vector-space is $1, X, X^2, X^3, \ldots$.

Q.6: Give a basis for the four-dimensional vector-space $\mathbb{F}_2^4$. What happens when an element of the vector-space is added to itself an even number of times? An odd number?

Q.7: Write the identity matrix of $\mathcal{M}_4(\mathbb{F}_2)$, the vector-space of matrices of dimension 4 over $\mathbb{F}_2$.

Q.8: In the following, we let $M = \begin{pmatrix}0 & 1 & 1 & 0\\ 1 & 1 & 0 & 0\\ 1 & 0 & 1 & 1\\ 0 & 0 & 0 & 1\end{pmatrix}$, $\vec{u} = \begin{pmatrix}1 & 1 & 0 & 1\end{pmatrix}$, $\vec{v} = \begin{pmatrix}1\\1\\1\\0\end{pmatrix}$ be respectively a matrix, a row vector, and a column vector of dimension four over $\mathbb{F}_2$.

Compute $\vec{u}M$ and $M\vec{v}$. Is M an invertible matrix?