A bit on information theory

A cryptosystem is unconditionally secure (*absoluutselt turvaline*) (wrt. a class of attacks) if no adversary (no matter what resources it has) can break it with the help of these attacks.

Let $\mathbf{X}$ be a random variable over the set X and $\mathbf{Y}$ a random variable over the set Y.

$\Pr[\mathbf{X} = x]$ denotes the probability that $\mathbf{X}$ gets the value $x \in X$.

$\Pr[\mathbf{X} = x, \mathbf{Y} = y]$ denotes the probability that $\mathbf{X}$ gets the value $x \in X$ and simultaneously $\mathbf{Y}$ gets the value $y \in Y$.

$\Pr[\mathbf{X} = x | \mathbf{Y} = y]$ denotes the probability that $\mathbf{X}$ gets the value x, given that $\mathbf{Y}$ got the value y.

$$\begin{aligned}\Pr[\mathbf{X} = x, \mathbf{Y} = y] = \Pr[\mathbf{Y} = y] \cdot \Pr[\mathbf{X} = x | \mathbf{Y} = y] \\ = \Pr[\mathbf{X} = x] \cdot \Pr[\mathbf{Y} = y | \mathbf{X} = x]\end{aligned}$$

Bayes' theorem: if $\Pr[\mathbf{Y} = y] > 0$, then

$$\Pr[\mathbf{X} = x | \mathbf{Y} = y] = \frac{\Pr[\mathbf{X} = x] \cdot \Pr[\mathbf{Y} = y | \mathbf{X} = x]}{\Pr[\mathbf{Y} = y]} \quad .$$

$\mathbf{X}$ ja $\mathbf{Y}$ are independent, if $\Pr[\mathbf{X} = x | \mathbf{Y} = y] = \Pr[\mathbf{X} = x]$ for all $x \in X$, $y \in Y$.

Let **P**, **K** ja **C** be random variables over sets $\mathcal{P}$, $\mathcal{K}$ ja $\mathcal{C}$, describing the distribution of plaintexts, keys and ciphertexts. Then

$$\Pr[\mathbf{C}=y] = \sum_{\substack{x\in\mathcal{P}\\ k\in\mathcal{K}\\ e_k(x)=y}} \Pr[\mathbf{P}=x,\mathbf{K}=k] =$$

$$\sum_{k\in\mathcal{K}} \Pr[\mathbf{P}=d_k(y),\mathbf{K}=k] = \sum_{k\in\mathcal{K}} \Pr[\mathbf{P}=d_k(y)]\cdot\Pr[\mathbf{K}=k] \ .$$

$$\Pr[\mathbf{C}=y|\mathbf{P}=x] = \sum_{\substack{k\in\mathcal{K}\\ y=e_k(x)}} \Pr[\mathbf{K}=k]$$

$$\Pr[\mathbf{P}=x|\mathbf{C}=y] = \frac{\Pr[\mathbf{P}=x]\cdot \sum\limits_{\substack{k\in\mathcal{K}\\ y=e_k(x)}} \Pr[\mathbf{K}=k]}{\sum\limits_{k\in\mathcal{K}} \Pr[\mathbf{P}=d_k(y)]\cdot\Pr[\mathbf{K}=k]}$$

An encryption system has perfect secrecy, if $\Pr[\mathbf{P} = x | \mathbf{C} = y] = \Pr[\mathbf{P} = x]$ for all $x \in \mathcal{P}$, $y \in \mathcal{C}$.

Equivalently: $\Pr[\mathbf{C} = y | \mathbf{P} = x] = \Pr[\mathbf{C} = y]$ for all $x \in \mathcal{P}$, $y \in \mathcal{C}$.

Perfect secrecy is unconditional security wrt. ciphertext-only attacks.

Theorem. Shift cipher has perfect secrecy if its key is chosen with uniform probability and a key is used to encrypt a single character.

Proof. $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$.

- $\Pr[\mathbf{K} = k] = 1/26$ for all $k \in \mathbb{Z}_{26}$.
- $\Pr[\mathbf{C} = y] = 1/26$ for all $y \in \mathbb{Z}_{26}$, because $y = x + k$, x and k are independent and k is uniformly distributed.
- $\Pr[\mathbf{C} = y | \mathbf{P} = x] = \Pr[\mathbf{K} = y - x] = 1/26$.

$$\Pr[\mathbf{P} = x | \mathbf{C} = y] = \frac{\Pr[\mathbf{P} = x] \cdot (1/26)}{1/26} = \Pr[\mathbf{P} = x] \ .$$

Assume that $\Pr[\mathbf{C} = y] > 0$ for all $y \in \mathcal{C}$. If not, then remove this y from $\mathcal{C}$.

Lemma. If a cryptosystem has perfect secrecy then for all $x \in \mathcal{P}$ and $y \in \mathcal{C}$ there exists $k \in \mathcal{K}$, such that $e_k(x) = y$.

Proof. Assume the contrary, i.e. there exist x and y, such that $e_k(x) = y$ for no k. Then $\Pr[\mathbf{C} = y | \mathbf{P} = x] = 0$, but $\Pr[\mathbf{C} = y] > 0$. Hence there is no perfect secrecy.

Theorem. Let $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ be an encryption system where $|\mathcal{P}| = |\mathcal{K}| = |\mathcal{C}|$. This encryption system has perfect secrecy iff the key is chosen uniformly and for all $x \in \mathcal{P}$, $y \in \mathcal{C}$ exists a unique $k \in \mathcal{K}$, such that $e_k(x) = y$.

Proof. $\Rightarrow$. Let the system have perfect secrecy. Then for all $x \in \mathcal{P}$ and $y \in \mathcal{C}$ there is at least one $k \in \mathcal{K}$, such that $e_k(x) = y$. Because the same key is usable for at most $|\mathcal{P}|$ pairs of (x, y), there cannot be more than one.

Fix $y \in \mathcal{C}$. Let $\mathcal{P} = \{x_1, \ldots, x_n\}$. Denote the elements of $\mathcal{K}$ in such a way: let $k_i \in \mathcal{K}$ be the key for which $e_{k_i}(x_i) = y$. From the perfect secrecy:

$$\Pr[\mathbf{P} = x_i] = \Pr[\mathbf{P} = x_i | \mathbf{C} = y] = \frac{\Pr[\mathbf{P} = x_i] \cdot \Pr[\mathbf{C} = y | \mathbf{P} = x_i]}{\Pr[\mathbf{C} = y]} = \frac{\Pr[\mathbf{P} = x_i] \cdot \Pr[\mathbf{K} = k_i]}{\Pr[\mathbf{C} = y]},$$

i.e. $\Pr[\mathbf{K} = k_i] = \Pr[\mathbf{C} = y]$ for all i, i.e. the probabilities of all keys must be equal.

$\Leftarrow$: like the proof of perfect secrecy for the shift cipher.

Vernam's cipher or one-time pad (*ühekordne šifriblokk*):

- $\mathcal{P} = \mathcal{C} = \mathcal{K} = \{0,1\}^n$;
- $e_{k_1 \ldots k_n}(x_1 \ldots x_n) = d_{k_1 \ldots k_n}(x_1 \ldots x_n) = (x_1 \oplus k_1) \ldots (x_n \oplus k_n)$.
  - $k_i, x_i \in \{0,1\}$.

Vernam's cipher has perfect secrecy (if the key is uniformly distributed and each key is used only once).

If we do not have perfect secrecy, then how much information about the key is leaked into the ciphertext? When can we determine the key (and the plaintext) with near-absolute certainty?

Let $\mathbf{X}$ be a random variable over the (finite) set X. The entropy of $\mathbf{X}$ is

$$H(\mathbf{X}) = -\sum_{x \in X} \Pr[\mathbf{X} = x] \cdot \log_2 \Pr[\mathbf{X} = x] \ .$$

Define $0 \cdot \log_2 0 = 0$, because $\lim_{x \to 0} x \log x = 0$.

$H(\mathbf{X})$ (more or less) corresponds to the average number of bits necessary to encode the value of $\mathbf{X}$.

$H(\mathbf{X}) = 0$ if and only if $\mathbf{X}$ always gets the same value. Then one of the probabilities is 1 and the rest are 0.

$$H(\mathbf{X}, \mathbf{Y}) = -\sum_{\substack{x \in X \\ y \in Y}} \Pr[\mathbf{X} = x, \mathbf{Y} = y] \cdot \log_2 \Pr[\mathbf{X} = x, \mathbf{Y} = y] \ .$$

Conditional entropy of $\mathbf{X}$ wrt. $\mathbf{Y}$:

$$H(\mathbf{X}|\mathbf{Y}) = -\sum_{y \in Y} \sum_{x \in X} \Pr[\mathbf{Y} = y] \Pr[\mathbf{X} = x | \mathbf{Y} = y] \log_2 \Pr[\mathbf{X} = x | \mathbf{Y} = y] \ .$$

How many bits are necessary to encode $\mathbf{X}$ if everybody knows $\mathbf{Y}$?

A function f is concave (*kumer*) in an interval $[a, b]$ if for all $x_1, x_2 \in [a, b]$ and $\lambda \in [0, 1]$:

$$\lambda \cdot f(x_1) + (1 - \lambda) \cdot f(x_2) \leq f(\lambda \cdot x_1 + (1 - \lambda) \cdot x_2) \ .$$

I.e. the graph of the function (in the interval $[a, b]$) is above any straight line segment between two points of that graph.

Concavity is strict (*range*) if equality holds only for $\lambda \in \{0, 1\}$ (whenever $x_1 \neq x_2$).

Logarithm is a strictly concave function in $[0, \infty)$...

Jensen's inequality: let f be strictly concave function in the interval I. Let $x_1, \ldots, x_n \in I$ and let $a_1, \ldots, a_n \in (0, 1]$, such that $a_1 + \cdots + a_n = 1$. Then

$$\sum_{i=1}^{n} a_i f(x_i) \leq f\Big(\sum_{i=1}^{n} x_i\Big)$$

and equality holds iff $x_1 = \cdots = x_n$.

Proof: induction over n. $n = 2$ is the def. of concavity.

Theorem. The maximum value of $H(\mathbf{X})$ is $\log_2 |X|$. It is attained only if $\mathbf{X}$ is uniformly distributed.

Proof. Let $X = \{x_1, \ldots, x_n\}$ and denote $p_i = \Pr[\mathbf{X} = x_i]$ Assume that $p_i > 0$ (otherwise remove x_i from X). Then $|X| = n$.

$$H(\mathbf{X}) = -\sum_{i=1}^{n} p_i \log_2 p_i = \sum_{i=1}^{n} p_i \log_2 \frac{1}{p_i} \leq \log_2 \sum_{i=1}^{n} p_i \cdot \frac{1}{p_i} = \log_2 n \ .$$

We used Jensen's inequality with $a_i = p_i$ and $x_i = 1/p_i$. The equality holds only if $1/p_1 = \cdots = 1/p_n$, i.e. $p_1 = \cdots = p_n$.

Theorem. $H(\mathbf{X}, \mathbf{Y}) \le H(\mathbf{X}) + H(\mathbf{Y})$ with equality holding iff $\mathbf{X}$ and $\mathbf{Y}$ are independent.

Proof. Let $X = \{x_1, \ldots, x_n\}$, $Y = \{y_1, \ldots, y_m\}$ and denote

- $p_i = \Pr[\mathbf{X} = x_i]$;
- $q_i = \Pr[\mathbf{Y} = y_i]$;
- $r_{ij} = \Pr[\mathbf{X} = x_i, \mathbf{Y} = y_i]$. Then
  - $p_i = \sum_{j=1}^{m} r_{ij}$,
  - $q_j = \sum_{i=1}^{n} r_{ij}$.

$\mathbf{X}$ and $\mathbf{Y}$ are independent iff $r_{ij} = p_i q_j$ for all i, j.

$$H(\mathbf{X},\mathbf{Y}) = -\sum_{i=1}^{n}\sum_{j=1}^{m} r_{ij}\log_2 r_{ij} = \sum_{i=1}^{n}\sum_{j=1}^{m} r_{ij}\log_2 \frac{1}{r_{ij}}$$

$$H(\mathbf{X}) + H(\mathbf{Y}) = -\sum_{i=1}^{n} p_i \log_2 p_i - \sum_{j=1}^{m} q_j \log_2 q_j =$$

$$-\left(\sum_{i=1}^{n}\sum_{j=1}^{m} r_{ij}\log_2 p_i + \sum_{j=1}^{m}\sum_{i=1}^{n} r_{ij}\log_2 q_j\right) =$$

$$-\sum_{i=1}^{n}\sum_{j=1}^{m} r_{ij}(\log_2 p_i + \log_2 q_j) = -\sum_{i=1}^{n}\sum_{j=1}^{m} r_{ij}\log_2(p_i q_j)$$

$$H(\mathbf{X},\mathbf{Y})-H(\mathbf{X})-H(\mathbf{Y}) = \sum_{i=1}^{n}\sum_{j=1}^{m} r_{ij}\log_2\frac{1}{r_{ij}}+\sum_{i=1}^{n}\sum_{j=1}^{m} r_{ij}\log_2(p_iq_j) =$$

$$\sum_{i=1}^{n}\sum_{j=1}^{m} r_{ij}\left(\log_2\frac{1}{r_{ij}}+\log_2(p_iq_j)\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} r_{ij}\log_2\frac{p_iq_j}{r_{ij}} \le$$

$$\log_2\sum_{i=1}^{n}\sum_{j=1}^{m} r_{ij}\cdot\frac{p_iq_j}{r_{ij}} = \log_2\sum_{i=1}^{n}\sum_{j=1}^{m} p_iq_j = \log_2\left(\sum_{i=1}^{n} p_i\right)\cdot\left(\sum_{j=1}^{m} q_j\right) = \log_2 1 = 0$$

We used Jensen's inequality with $a_{ij} = r_{ij}$ and $x_{ij} = p_iq_j/r_{ij}$.

Equality holds only if $\exists c\,\forall i\,\forall j : p_iq_j/r_{ij} = c$. Then also $\sum\limits_{i=1}^{n}\sum\limits_{j=1}^{m} p_iq_j = c\sum\limits_{i=1}^{n}\sum\limits_{j=1}^{m} r_{ij}$. Both sums are equal to 1, hence $c = 1$, $p_iq_j = r_{ij}$, and $\mathbf{X}$ and $\mathbf{Y}$ are independent.

Theorem. $H(\mathbf{X}, \mathbf{Y}) = H(\mathbf{Y}) + H(\mathbf{X}|\mathbf{Y})$.

Proof. Let p_i, q_j, r_{ij} have the same meaning as before. Then

$$\Pr[\mathbf{X} = x_i | \mathbf{Y} = y_j] = \frac{\Pr[\mathbf{X} = x_i, \mathbf{Y} = y_j]}{\Pr[\mathbf{Y} = y_j]} = \frac{r_{ij}}{q_j} \quad .$$

$$H(\mathbf{Y}) + H(\mathbf{X}|\mathbf{Y}) = -\sum_{j=1}^{m} q_j \log_2 q_j - \sum_{i=1}^{n}\sum_{j=1}^{m} q_j \frac{r_{ij}}{q_j} \log_2 \frac{r_{ij}}{q_j} =$$

$$-\left(\sum_{i=1}^{n}\sum_{j=1}^{m} r_{ij} \log_2 q_j + \sum_{i=1}^{n}\sum_{j=1}^{m} r_{ij} \log_2 \frac{r_{ij}}{q_j}\right) =$$

$$-\sum_{i=1}^{n}\sum_{j=1}^{m} r_{ij} \log_2 r_{ij} = H(\mathbf{X}, \mathbf{Y})$$

Corollary. $H(\mathbf{X}|\mathbf{Y}) \leq H(\mathbf{X})$ with equality iff $\mathbf{X}$ and $\mathbf{Y}$ are independent.

Theorem. In an encryption system, $H(\mathbf{K}|\mathbf{C}) = H(\mathbf{K}) + H(\mathbf{P}) - H(\mathbf{C})$.

Proof.

$$H(\mathbf{K}|\mathbf{C}) = H(\mathbf{K},\mathbf{C}) - H(\mathbf{C}) = H(\mathbf{P},\mathbf{K},\mathbf{C}) - H(\mathbf{P}|\mathbf{K},\mathbf{C}) - H(\mathbf{C}) =^{1)}$$
$$H(\mathbf{P},\mathbf{K},\mathbf{C}) - H(\mathbf{C}) = H(\mathbf{P},\mathbf{K}) + H(\mathbf{C}|\mathbf{P},\mathbf{K}) - H(\mathbf{C}) =^{2)}$$
$$H(\mathbf{P},\mathbf{K}) - H(\mathbf{C}) =^{3)} H(\mathbf{P}) + H(\mathbf{K}) - H(\mathbf{C})$$

1. Ciphertext and key uniquely determine the plaintext, hence $H(\mathbf{P}|\mathbf{K},\mathbf{C}) = 0$.
2. Similarly, $H(\mathbf{C}|\mathbf{P},\mathbf{K}) = 0$.
3. Plaintext and key are independent — the key has been chosen beforehand and it should not influence the choice of the plaintext.

We know how to compute $H(\mathbf{K})$. But what is $H(\mathbf{P})$? How to estimate it? The possible values of $\mathbf{P}$ are meaningful texts. $\mathcal{P}$ is the set of strings over an alphabet (of, say, 26 letters).

The entropy of a random string of letters (uniformly chosen) is $\log_2 26 \approx 4.70$ per letter.

The entropy of a random string of letters (with probabilities of letters as in English) is ≈ 4.17 per letter.

But in a meaningful text, successive letters are not independent.

Let $\mathbf{P}^n$ be a random variable that ranges over plaintexts of length n with probabilities of the natural language L.

If we have a large enough corpus of texts then we can compute $\Pr[\mathbf{P}^n = s]$ for all $s \in \Sigma^n$, and also compute $H(\mathbf{P}^n)$.

Let $\mathbf{C}^n$ be the random variable ranging over n-letter ciphertexts.

The entropy H_L (per letter) and the redundancy R_L of L are

$$H_L = \lim_{n \to \infty} \frac{H(\mathbf{P}^n)}{n} \qquad\qquad R_L = 1 - \frac{H_L}{\log_2 |\Sigma|}$$

The limit exists because $(H(\mathbf{P}_n)/n)_n$ is a decreasing sequence bounded below by 0.

Various experiments estimate that $1.0 \leq H_{\text{English}} \leq 1.5$.

We have $H(\mathbf{P}^n) \geq nH_L = n(1 - R_L)\log_2|\Sigma|$ and $H(\mathbf{C}^n) \leq n\log_2|\Sigma|$. Hence

$$H(\mathbf{K}|\mathbf{C}^n) = H(\mathbf{K}) + H(\mathbf{P}^n) - H(\mathbf{C}^n) \geq H(\mathbf{K}) - nR_L\log_2|\Sigma| \ .$$

If the encryption key is chosen uniformly then

$$H(\mathbf{K}|\mathbf{C}^n) \geq \log_2|\mathcal{K}| - nR_L\log_2|\Sigma| = \log_2\frac{|\mathcal{K}|}{|\Sigma|^{nR_L}}$$

This inequality gives us some guarantees regarding the impossibility of completely determining the key from a ciphertext. This guarantee vanishes if

$$\log_2\frac{|\mathcal{K}|}{|\Sigma|^{nR_L}} \leq 0 \Leftrightarrow |\mathcal{K}| \leq |\Sigma|^{nR_L} \Leftrightarrow n \geq \frac{\log_2|\mathcal{K}|}{R_L\log_2|\Sigma|}$$

If we take $|\Sigma| = 26$, $|\mathcal{K}| = 26!$ (substitution cipher) and $R_L = 0.75$ (corresponding to $H_L \approx 1.18$) then the last fraction is ≈ 25.07. I.e. a ciphertext created using the substitution cipher should be uniquely decryptable if its length is at least 25.

Pisut arvuteooriat

(see, mida DME raamatus ei olnud)

Eukleidese algoritm $\gcd(a, b)$ leidmiseks, kus $a, b \in \mathbb{N}\backslash\{0\}$:

Loeme, et $a \geq b$. Olgu $a_0 = a$ ja $a_1 = b$. Iga $n \geq 1$ jaoks olgu $a_{n+1} = a_{n-1} \bmod a_n$, kui $a_n \neq 0$. Siis $\gcd(a, b)$ on võrdne viimase 0-st erineva elemendiga järjendis (a_n).

Lemma. Eukleidese algoritm on korrektne.

Tõestus. Induktsioon üle järjendi (a_n) pikkuse.

Baas: $a_2 = 0$. Siis $b \,|\, a$ ning $\gcd(a, b) = b = a_1$.

Samm: Näitame, et $\gcd(a, b) = \gcd(b, a \bmod b)$.

I) Olgu $d \,|\, a$ ja $d \,|\, b$. Siis $a \bmod b = a - b \cdot \lfloor a/b \rfloor = d\big((a/d) - (b/d) \cdot \lfloor a/b \rfloor\big)$.

II) Olgu $d \,|\, b$ ja $d \,|\, (a \bmod b)$. Siis $a = b \cdot \lfloor a/b \rfloor + (a \bmod b) = d\big((b/d) \cdot \lfloor a/b \rfloor + (a \bmod b)/d\big)$.

Lemma. Olgu (a_n) järjend, mis tekib Eukleidese algoritmi kasutamisel $\gcd(a,b)$ leidmiseks. Siis iga n jaoks leiduvad $u_n, v_n \in \mathbb{Z}$ nii, et $u_n a + v_n b = a_n$.

Tõestus. $u_0 = 1$, $v_0 = 0$, $u_1 = 0$, $v_1 = 1$.

Järjendis (a_n) kehtib

$$a_{n+1} = a_{n-1} - a_n \cdot \lfloor a_{n-1}/a_n \rfloor \ .$$

Võtamegi siis

$$\begin{aligned} u_{n+1} &= u_{n-1} - u_n \cdot \lfloor a_{n-1}/a_n \rfloor \\ v_{n+1} &= v_{n-1} - v_n \cdot \lfloor a_{n-1}/a_n \rfloor \ . \end{aligned}$$

Muuhulgas, kui $\gcd(a,n) = 1$, siis leiduvad $u, v \in \mathbb{Z}$ nii, et $ua + vn = 1$. Ringis $\mathbb{Z}_n$ siis $ua = 1$, s.t. $u = a^{-1} \pmod{n}$.

Hulk $\mathbb{Z}_n^*$

…on struktuuri $(\mathbb{Z}_n, \cdot)$ kõigi pööratavate elementide hulk:

$$\begin{aligned} \mathbb{Z}_n^* &= \{x \in \mathbb{Z}_n : \exists x' \in \mathbb{Z}_n, x \cdot x' = 1\} = \\ &= \{x \in \mathbb{Z}_n : \gcd(x, n) = 1\}. \end{aligned}$$

Teoreem. Struktuur $(\mathbb{Z}_n^*, \cdot)$ on rühm.

Millised paarid (k, a) sobivad afiinse šifri

$$\mathbb{Z}_n \to \mathbb{Z}_n : x \mapsto k \cdot x + a \mod n$$

võtmeteks, et see šiffer oleks pööratav? Ilmselt

$$(k, a) \in \mathbb{Z}_n^* \times \mathbb{Z}_n.$$

Kui suur on võtmeruum?

$$|\mathbb{Z}_n^* \times \mathbb{Z}_n| = |\mathbb{Z}_n^*| \cdot |\mathbb{Z}_n| = |\mathbb{Z}_n^*| \cdot n.$$

Euleri φ-funktsioon

...on defineeritud kui

$$\varphi(n) := |\mathbb{Z}_n^*| = |\{x \in \mathbb{Z}_n : \gcd(x,n) = 1\}|.$$

Teoreem. Olgu $p \in \mathbb{P}$ ja $e \in \mathbb{N}$. Siis

$$\varphi(p^e) = p^e - p^{e-1}.$$

Kuidas avaldub $\varphi(n)$ suvalise $n \in \mathbb{N}$ jaoks? Teame, et n-i saab esitada algtegurite astmete korrutisena:

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}.$$

Teoreem.

$$\varphi(n) = (p_1^{e_1} - p_1^{e_1-1}) \cdot \ldots \cdot (p_r^{e_r} - p_r^{e_r-1}).$$

See teoreem järeldub järgmisest lemmast.

Lemma. Kui $\gcd(m,n) = 1$, siis

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n).$$

$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$: **näide**

Vaatleme juhtu $n = 72$.

$$\begin{aligned}
\varphi(72) &= \varphi(8 \cdot 9) = \varphi(8) \cdot \varphi(9) = \\
&= \varphi(2^3) \cdot \varphi(3^2) = (2^3 - 2^2) \cdot (3^2 - 3^1) = \\
&= (8 - 4) \cdot (9 - 3) = 4 \cdot 6 = 24.
\end{aligned}$$

	0	1	2	3	4	5	6	7	8
0	0	64	56	48	40	32	24	16	8
1	9	1	65	57	49	41	33	25	17
2	18	10	2	66	58	50	42	34	26
3	27	19	11	3	67	59	51	43	35
4	36	28	20	12	4	68	60	52	44
5	45	37	29	21	13	5	69	61	53
6	54	46	38	30	22	14	6	70	62
7	63	55	47	39	31	23	15	7	71

Tõestuse skeem (I)

Kui $\gcd(m,n)=1$, siis on kujutus

$$CRT : \mathbb{Z}_{m\cdot n} \to \mathbb{Z}_m \times \mathbb{Z}_n : x \mapsto (x \mod m, x \mod n)$$

bijektsioon. See väide on samaväärne *Hiina jäägiteoreemiga.*

Teoreem. Kui $\gcd(m,n)=1$, siis on kongruentside süsteemil

$$\begin{aligned} x &= a \mod m, \\ x &= b \mod n \end{aligned}$$

täpselt üks lahend modulo $m\cdot n$.

Hiina jäägiteoreem (üldkujul)

Teoreem. Olgu $m_1, m_2, \ldots, m_r$ paarikaupa ühistegurita naturaalarvud ja $a_1, a_2, \ldots, a_r$ mingid naturaalarvud. Siis on süsteemil

$$\begin{aligned} x &= a_1 \mod m_1 \\ x &= a_2 \mod m_2 \\ &\ldots \\ x &= a_r \mod m_r \end{aligned}$$

täpselt üks lahend modulo $m_1 \cdot m_2 \cdot \ldots \cdot m_r$.

Tõestus. x-i leiame järgmiselt. Olgu

- $M = m_1 \cdot m_2 \cdot \ldots \cdot m_r$.
- $M_i = M/m_i$, $1 \le i \le r$.
- $M'_i = M_i^{-1} \pmod{m_i}$.
- $x = (M_1 M'_1 a_1 + M_2 M'_2 a_2 + \ldots + M_r M'_r a_r) \bmod M$.

Siis $x \equiv M_i M'_i a_i \equiv a_i \pmod{m_i}$, sest $M_j \equiv 0 \pmod{m_i}$, kui $i \neq j$.

Näitasime, et leidub vähemalt üks lahend. Seega on kujutus CRT sürjektiivne. Injektiivsus järeldub määramis- ja muutumispiirkonna võimsuste võrdsusest ja lõplikusest.

Tõestuse skeem (II)

Väite

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$$

ehk

$$|\mathbb{Z}^*_{m \cdot n}| = |\mathbb{Z}^*_m| \cdot |\mathbb{Z}^*_n| (= |\mathbb{Z}^*_m \times \mathbb{Z}^*_n|)$$

tõestamiseks piisab tõestada, et

$$x \in \mathbb{Z}^*_{m \cdot n} \Leftrightarrow CRT(x) \in \mathbb{Z}^*_m \times \mathbb{Z}^*_n.$$

Olgu $x \in \mathbb{Z}^*_{m \cdot n}$. Olgu y selline, et $xy \equiv 1 \pmod{m \cdot n}$. Siis $xy \equiv 1 \pmod{m}$ ja $xy \equiv 1 \pmod{n}$.

Olgu $y \in \mathbb{Z}^*_m$ ja $z \in Z^*_n$. Olgu $x \in \mathbb{Z}_{m \cdot n}$ selline, et $x \bmod m = y$ ja $x \bmod n = z$. Olgu y', z' sellised, et $yy' \equiv 1 \pmod{m}$ ja $zz' \equiv 1 \pmod{n}$. Olgu $x' \in \mathbb{Z}_{m \cdot n}$ selline, et $x' \equiv y' \pmod{m}$ ja $x' \equiv z' \pmod{n}$. Siis $xx' \equiv yy' \equiv 1 \pmod{m}$ ja $xx' \equiv zz' \equiv 1 \pmod{n}$. Seega $xx' \equiv 1 \pmod{m \cdot n}$.

Blokkšifrite töörežiimid

Krüptosüsteemi definitsioon

Definitsioon 1 Krüptosüsteemiks *nimetame viisikut* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, *kus*

1. $\mathcal{P}$ *on kõigi võimalike avatekstide hulk;*
2. $\mathcal{C}$ *on kõigi võimalike krüptotekstide hulk;*
3. $\mathcal{K}$ *on kõigi võimalike võtmete hulk;*
4. $\forall K \in \mathcal{K}\ \exists e_K \in \mathcal{E}$, $d_K \in \mathcal{D}$, $e_K : \mathcal{P} \to \mathcal{C}$, $d_K : \mathcal{C} \to \mathcal{P}$:

$$\forall x \in \mathcal{P}\ d_K(e_K(x)) = x.$$

Nihkešiffer kui krüptosüsteem

Nihkešifri korral $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$, kodeerimisreegel on

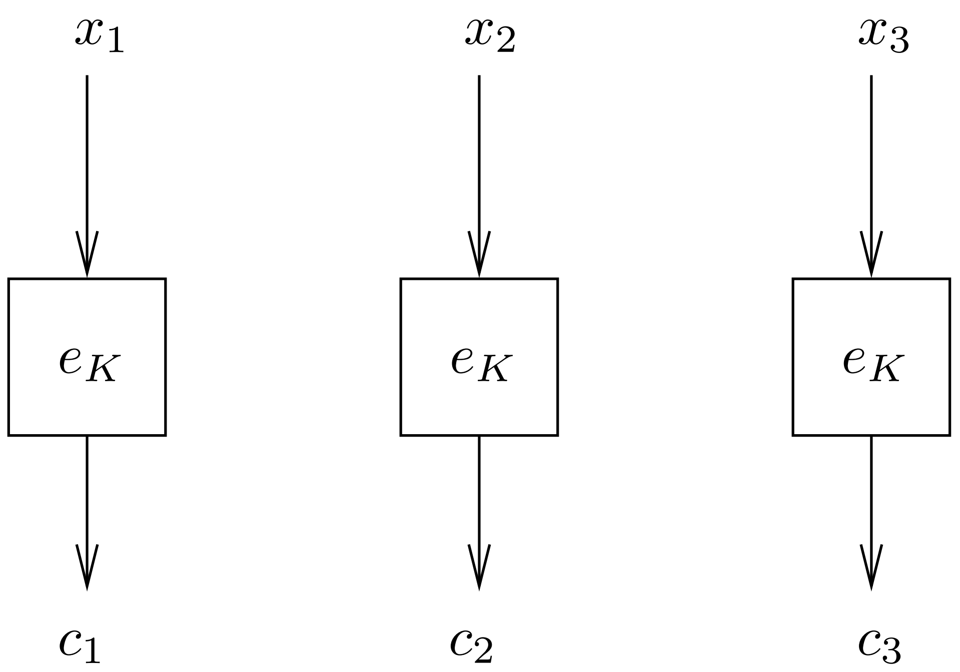
$$e_K : x_1 x_2 \dots x_n \mapsto (x_1 + K)(x_2 + K) \dots (x_n + K)$$

ning dekodeerimisreegel

$$d_K : x_1 x_2 \dots x_n \mapsto (x_1 - K)(x_2 - K) \dots (x_n - K).$$

Niisugust krüptosüsteemi, mis jagab teksti blokkideks ja kodeerib kõik blokid ühtmoodi, nimetatakse *blokkšifriks*.

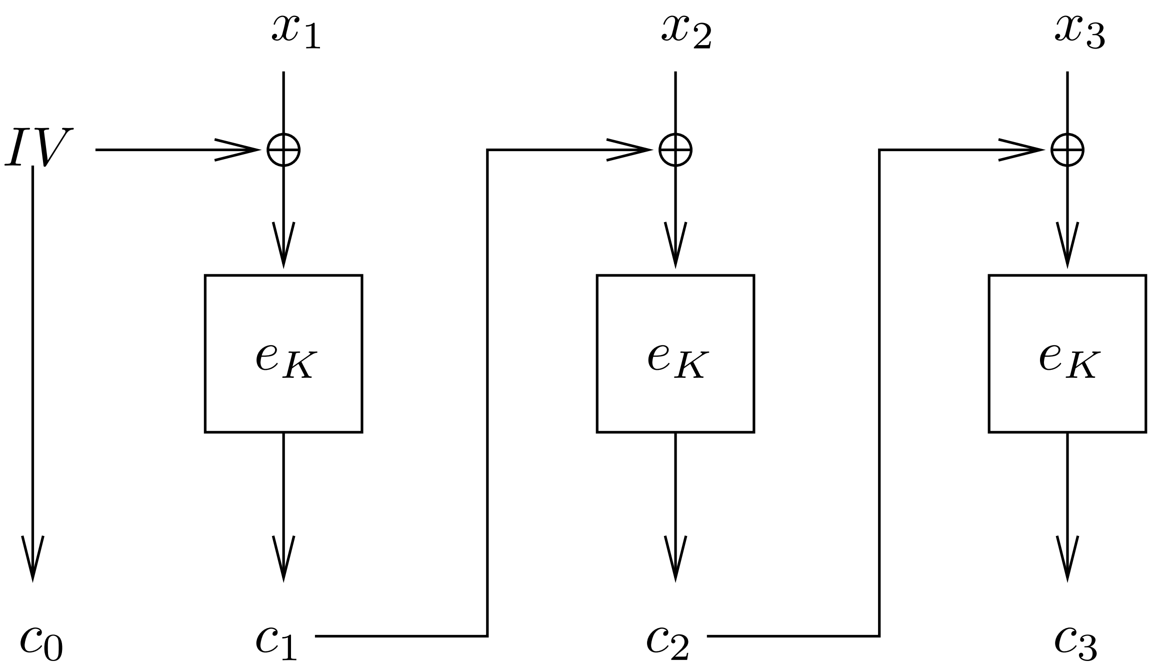
Blokkšifrite töörežiimid: ECB



ECB-režiimi omadused

1. Identsed avatekstiblokid kodeeruvad sama võtmega identseteks krüptotekstiblokkideks.
2. Krüptotekstiblokkide ümberjärjestamisel saadakse vigadeta dekodeeruv krüptotekst.
3. Mõne krüptotekstibloki bitivead ei mõjuta teisi blokke.

Blokkšifrite töörežiimid: CBC



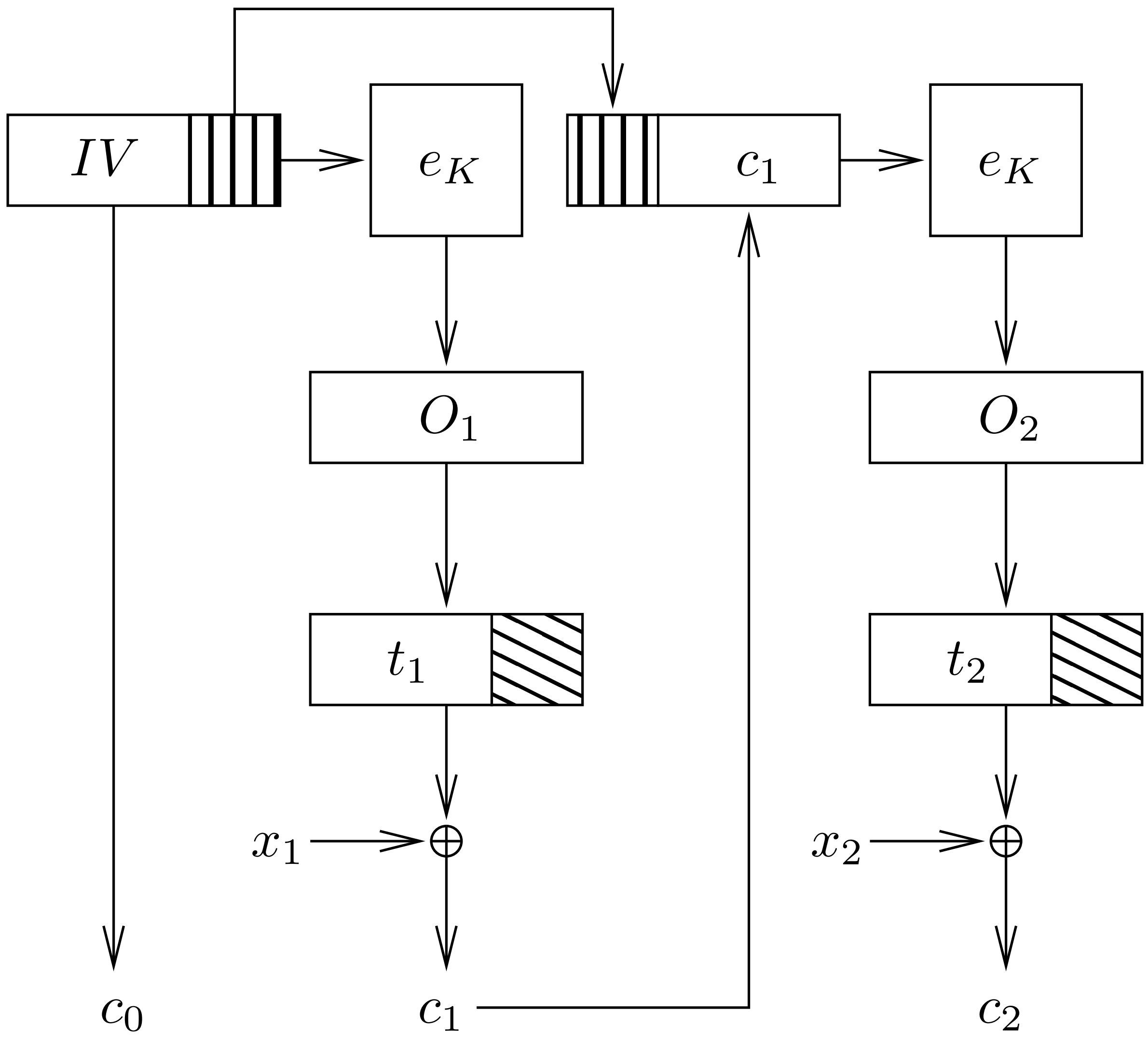
CBC-režiimi omadused

1. Kui sama avateksti kodeerida mitu korda erinevate IV väärtustega, on tulemuseks erinev krüptotekst.

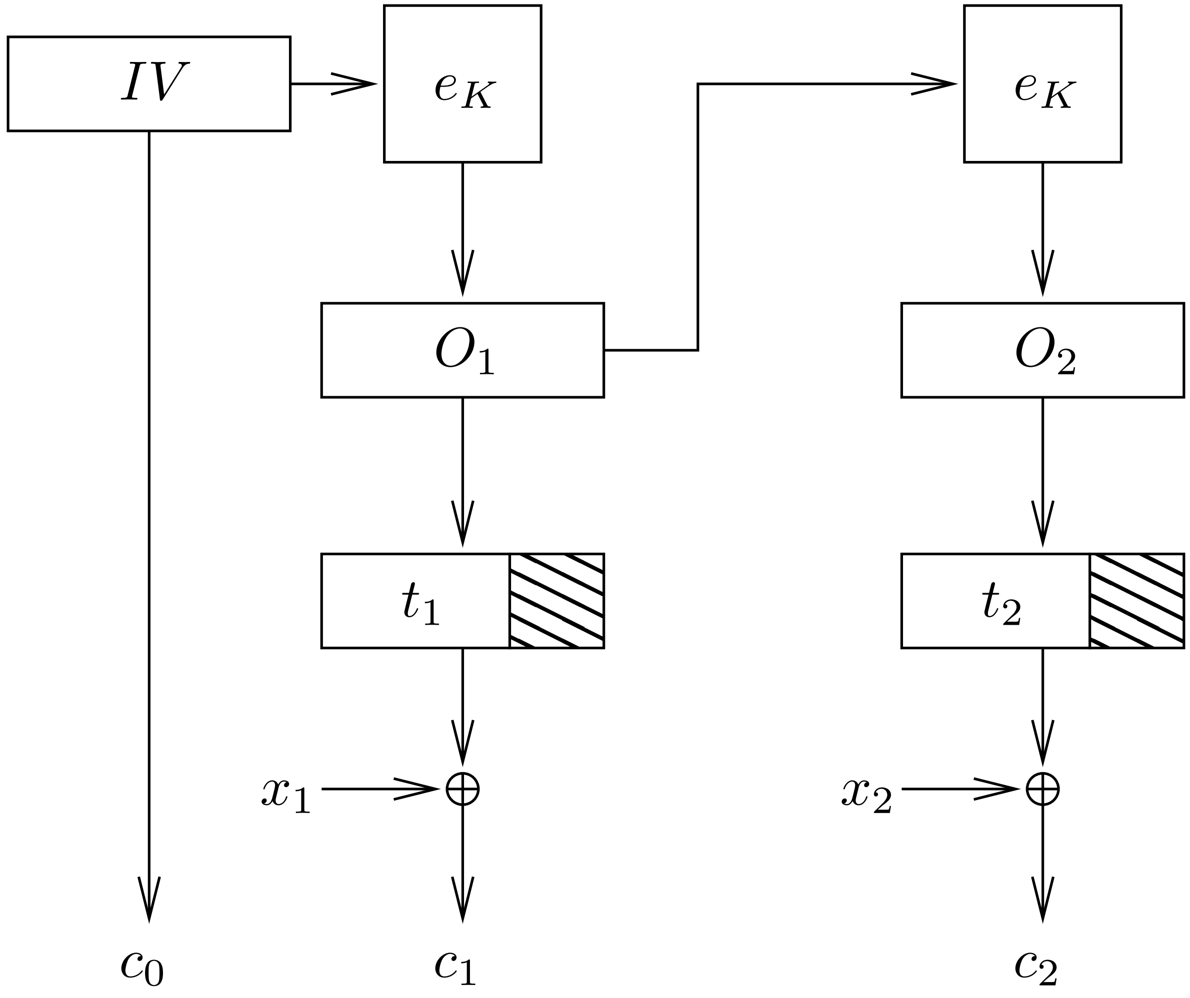
2. Kuna iga kodeeritav blokk mõjutab kõiki järgmisi, ei saa ründaja krüptoteksti blokke avastamatult ümber paigutada. Küll aga võib ründaja krüptoteksti lõpust suvalise koguse blokke kustutada.

3. Kui krüptoteksti blokis c_i esinevad bitivead, mõjutavad need ainult i. ja $(i+1)$. bloki dekodeerimist. Saadav blokk x'_i näeb siis reeglina välja juhuslik, kuid $(i+1)$. avateksti blokis esinevad vead täpselt nendel positsioonidel kus i. krüptotekstiblokiski.

Blokkšifrite töörežiimid: CFB



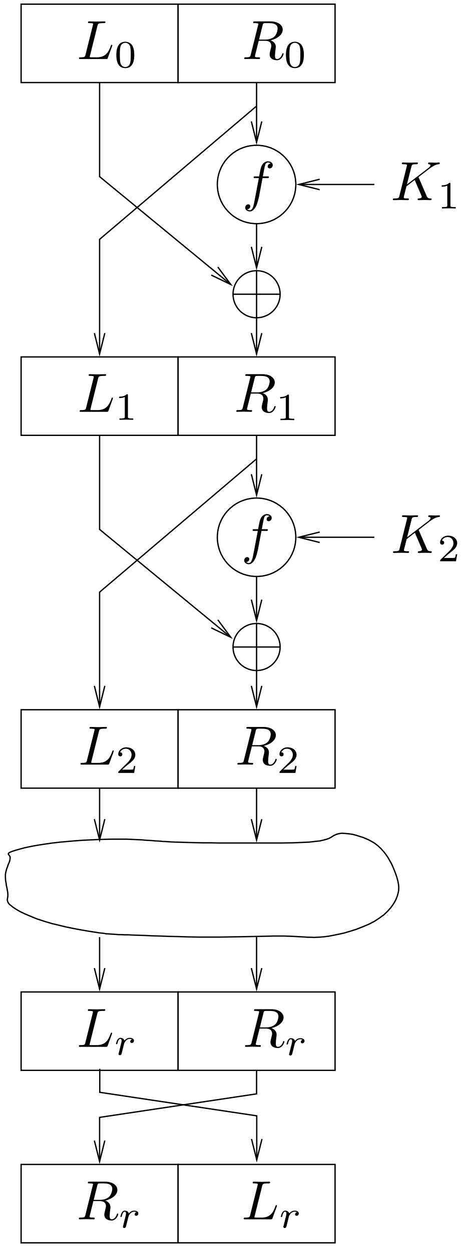
Blokkšifrite töörežiimid: OFB



CFB ja OFB-režiimide omadused

. . . on kodune ülesanne.

Feisteli šifrid



- Üks võimalikke plokkšifrite konstruktsioone.
- Definitsioon peab spetsifitseerima funktsiooni f ja raundide arvu r.
- $K_1, \ldots, K_r$ on osavõtmed, need leitakse mingil viisil krüptosüsteemi võtmest K.
  – Krüptosüsteemi võti ei ole tavaliselt $K_1 \cdots K_r$, sest see oleks liiga pikk.

Ülesanded

1. Tõesta, et Feisteli šifrit saab dekodeerida kodeerimisalgoritmiga, rakendades alamvõtmeid järjekorras $K_r, K_{r-1}, \ldots, K_1$.

2. Analüüsi Feisteli šifri turvalisust, kui raundifunktsioon f töötab järgmiselt:

   (a) $f \equiv 0$,

   (b) $f(R, K) = R$.

Krüptosüsteemide korrutis

Definitsioon 2 *Krüptosüsteemi nimetame* endomorfseks, *kui* $\mathcal{P} = \mathcal{C}$.

Definitsioon 3 *Olgu meil kaks endomorfset krüptosüsteemi* $\mathbf{S}_1 = (\mathcal{P}, \mathcal{P}, \mathcal{K}_1, \mathcal{E}_1, \mathcal{D}_1)$ *ja* $\mathbf{S}_2 = (\mathcal{P}, \mathcal{P}, \mathcal{K}_2, \mathcal{E}_2, \mathcal{D}_2)$. *Nende* korrutiseks *nimetatakse krüptosusteemi*

$$\mathbf{S}_1 \times \mathbf{S}_2 = (\mathcal{P}, \mathcal{P}, \mathcal{K}_1 \times \mathcal{K}_2, \mathcal{E}, \mathcal{D}).$$

Võtmele $K = (K_1, K_2)$ *vastavad kodeerimis- ja dekoderimisreeglid on*

$$\begin{aligned} e_{(K_1,K_2)}(x) &= e_{K_2}(e_{K_1}(x)), \\ d_{(K_1,K_2)}(x) &= d_{K_1}(d_{K_2}(x)). \end{aligned}$$

Ülesanded

Olgu $\mathbf{N}$ nihkešiffer, $\mathbf{M}$ multiplikatiivne šiffer ja $\mathbf{A}$ afiinne šiffer tähestikul $\mathbb{Z}_{26}$. Tõesta, et

1. $\mathbf{N} \times \mathbf{N} \equiv \mathbf{N}$,
2. $\mathbf{M} \times \mathbf{M} \equiv \mathbf{M}$,
3. $\mathbf{M} \times \mathbf{N} \equiv \mathbf{N} \times \mathbf{M} \equiv \mathbf{A}$,
4. $\mathbf{A} \times \mathbf{A} \equiv \mathbf{A}$.

Multiplikatiivne šiffer: sama, mis nihkešiffer, aga võtit mitte ei liideta avateksti tähtedele, vaid korrutatakse. Võti peab siis kuuluma hulka $\mathbb{Z}_{26}^*$.

Võtmeruumi tõenäosusjaotus

Definitsioon 4 Tõenäosusjaotuseks *(lõplikul) hulgal* X *nimetame funktsiooni*

$$p : X \to [0,1],$$

mis rahuldab tingimust

$$\sum_{x \in X} p(x) = 1.$$

Ütleme, et jaotus on ühtlane, *kui iga* $x \in X$ *korral* $p(x) = \frac{1}{|X|}$.

Korrutisruumi tõenäosusjaotus

Olgu meil kaks krüptosüsteemi ning nende võtmeruumidel $\mathcal{K}_1$ ja $\mathcal{K}_2$ antud tõenäosusjaotused $p_{\mathcal{K}_1}$ ja $p_{\mathcal{K}_2}$. Korrutissüsteemi tõenäosusjaotus võtmeruumil $\mathcal{K} = \mathcal{K}_1 \times \mathcal{K}_2$ määratakse ära reegliga

$$p_{\mathcal{K}}(K_1, K_2) = p_{\mathcal{K}_1}(K_1) \cdot p_{\mathcal{K}_2}(K_2).$$

Ülesanne. Tõesta, et funktsioon p on tõepoolest tõenäosusjaotus.

Ülesanded

1. Tõesta, et kui kahe krüptosüsteemi võtmeruumid on ühtlase tõenäosusjaotusega, siis on see õige ka nende süsteemide korrutise jaoks. Kas kehtib ka vastupidine väide?

2. Vaatleme *one-time pad* krüptosüsteemi, kus kodeeritakse üks bitt, mis tõenäosusega p on 1, tõenäosusega $1-p$ aga 0. Tõesta, et kui võtmebitt on ühtlase jaotusega, siis on ühtlase jaotusega ka väljundbitt.

3. Olgu g rühmast G ühtlase jaotusega valitud element.
   (a) Tõesta, et g^{-1} on ühtlase jaotusega.
   (b) Tõesta, et suvalise jaotusega elemendi $h \in G$ korral on element $g \cdot h$ ühtlase jaotusega.

   Tee järeldus šifrite **N** ja **M** jaoks.