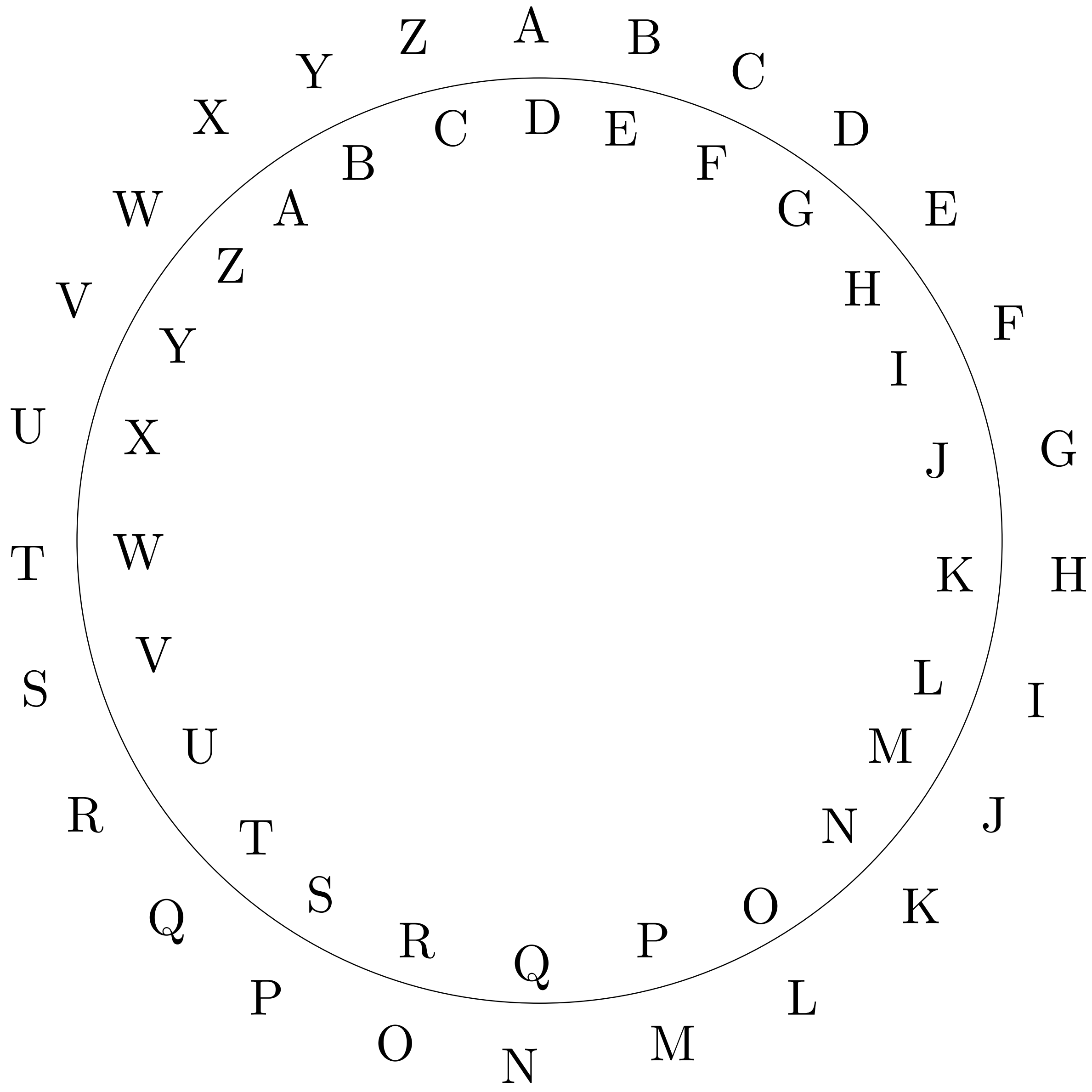
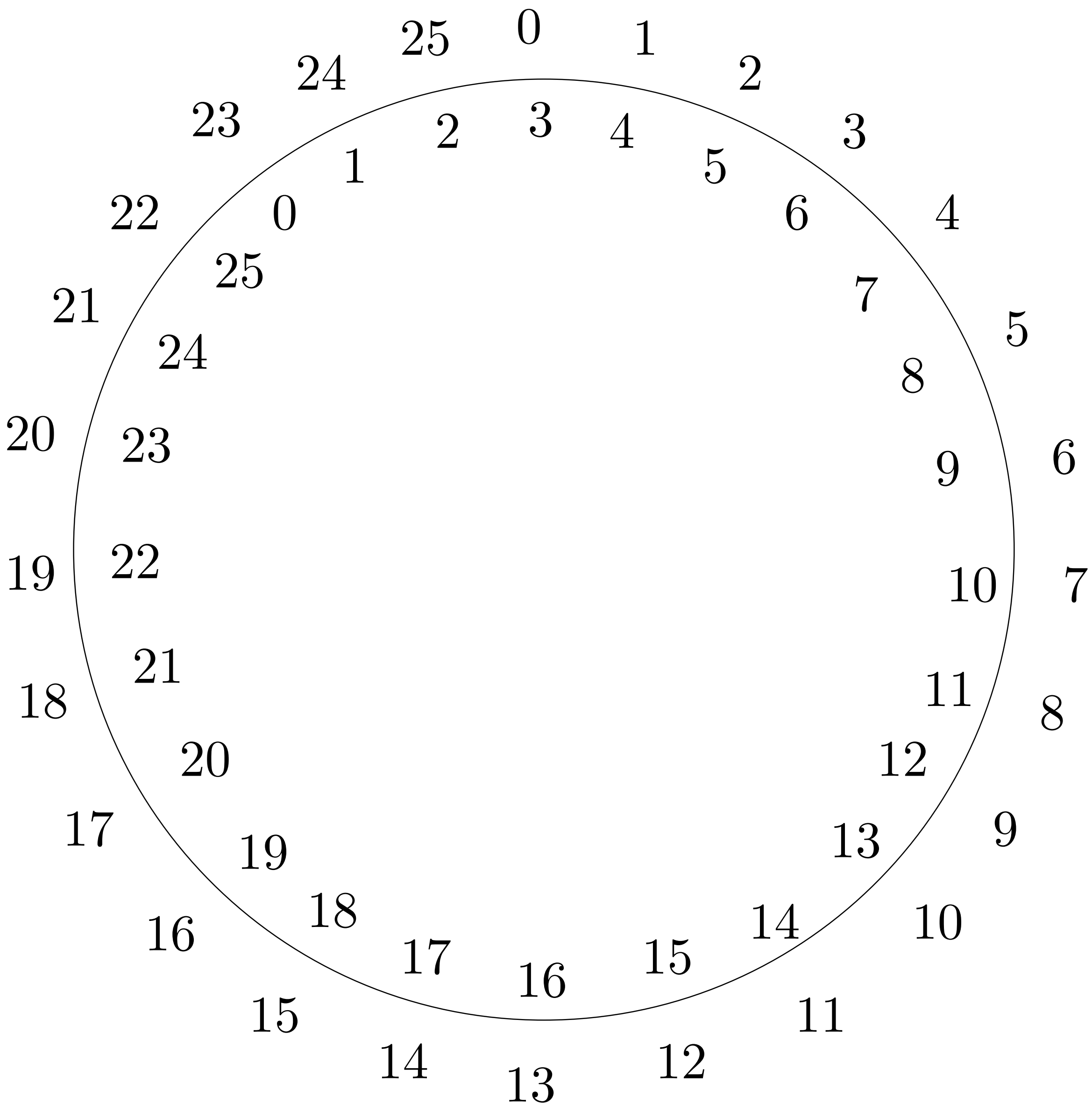
Caesari šiffer


A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Kuidas oleks seda šifrit mugav matemaatiliselt analüüsida?

Caesari šifri matemaatiline kuju



Asendame hulga $\{\mathrm{A}, \mathrm{B}, \mathrm{C}, \ldots, \mathrm{Y}, \mathrm{Z}\}$ hulgaga $\{0, 1, 2, \ldots, 24, 25\}$.

Arvutused jääkidega: liitmine

Vaatleme nende jääkide hulka, mis võivad tekkida jagamisel arvuga n:

$$\{0, 1, 2, \ldots, n-2, n-1\} := \mathbb{Z}_n.$$

Definerime hulgal $\mathbb{Z}_n$ liitmise: kui $a, b \in \mathbb{Z}_n$, siis

$$a \oplus b = a + b \mod n.$$

Edaspidi kirjutame $\oplus$ asemel lihtsalt $+$. Näiteks

$$\begin{aligned} 13 + 8 &= 21 \mod 26, \\ 13 + 8 &= 3 \mod 9. \end{aligned}$$

Caesari šiffer avaldub siis kujul

$$\mathbb{Z}_{26} \to \mathbb{Z}_{26} : x \mapsto x + 3 \mod 26$$

ja üldine *nihkešiffer* kujul

$$\mathbb{Z}_{26} \to \mathbb{Z}_{26} : x \mapsto x + a \mod 26.$$

Liitmise omadused

1. *Leidub ühikelement:*

   $$\exists o \in \mathbb{Z}_n \forall x \in \mathbb{Z}_n \;\; o + x = x + o = x \mod n$$

   Nihkešifri jaoks: leidub nihe, mis jätab kõik paigale. Ilmselt $o = 0$.

2. *Leiduvad pöördelemendid:*

   $$\forall x \in \mathbb{Z}_n \exists x' \in \mathbb{Z}_n \;\; x + x' = x' + x = o \mod n$$

   Nihkešifri jaoks: iga nihke jaouks leidub teine nihe, mis esimese annulleerib. Teisisõnu: iga kodeerimine nihkešifriga on dekodeeritav.

3. *Assotsiatiivsus:*

   $$\forall x, a, b \in \mathbb{Z}_n \;\; (x + a) + b = x + (a + b) \mod n$$

   Nihkešifri jaoks: me saame sama tulemuse, kui teeme järjest nihked a ja b võrra või kohe ühe nihke $a + b$ võrra.

Omaduste 1.–3. tõttu nimetatakse paari $(\mathbb{Z}_n, +)$ *(jäägiklassi)rühmaks*.

Arvutused jääkidega: korrutamine

Hulgas $\mathbb{Z}_n$ saab ka korrutada:

$$a \odot b = a \cdot b \mod n.$$

Edaspidi kirjutame $\odot$ asemel lihtsalt $\cdot$. Näiteks

$$\begin{aligned} 13 \cdot 8 &= 0 \mod 26, \\ 13 \cdot 8 &= 5 \mod 9. \end{aligned}$$

Siis saame defineerida *multiplikatiivse šifri*

$$\mathbb{Z}_{26} \to \mathbb{Z}_{26} : x \mapsto k \cdot x \mod 26$$

ja *afiinse šifri*

$$\mathbb{Z}_{26} \to \mathbb{Z}_{26} : x \mapsto k \cdot x + a \mod 26.$$

Korrutamise omadused

1. *Leidub ühikelement:*

$$\exists e \in \mathbb{Z}_n \forall x \in \mathbb{Z}_n \;\; e \cdot x = x \cdot e = x \mod n$$

   Selleks elemendiks sobib (ainsana) $e = 1$.

2. *Assotsiatiivsus:*

$$\forall x, a, b \in \mathbb{Z}_n \;\; (x \cdot a) \cdot b = x \cdot (a \cdot b) \mod n$$

Korrutamise suhtes ei pruugi alati pöördelementi leiduda, nt

$$\forall x \in \mathbb{Z}_n \;\; x \cdot 0 = 0,$$

järelikult ei leidu sellist elementi $0'$, et $0' \cdot 0 = 1$.

Seega ei ole multiplikatiivne ja afiinne šiffer alati pööratavad.

Aga millal on?

$(\mathbb{Z}_{10}, \cdot)$ pööratavad elemendid

	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

Teoreem. Korrutamise suhtes on pööratavad parajasti need elemendid $x \in \mathbb{Z}_n$, mille korral $\gcd(x, n) = 1$.

Definitsioon. Ringi R element $x \neq 0$ on nullitegur, kui leidub $y \in R$, $y \neq 0$ nii, et $x \cdot y = 0$.

Fakt. $0 \in R$ ei ole R-s pööratav.

Lemma. Nullitegur $x \in R$ ei ole R-s pööratav.

Tõestus. Olgu $y \in R$, $y \neq 0$ selline, et $xy = 0$. Siis

$$y = 1 \cdot y = x^{-1}xy = x^{-1} \cdot 0 = 0 \ .$$

Fakt. $1 \in R$ on pööratav.

Olgu $R^* \subset R$ ringi R kõigi pööratavate elementide hulk.

Lemma. Lõplikus ringis R leidub ainult kolme sorti elemente — 0, nullitegurid ja pööratavad elemendid.

Tõestus. Näitame, et kui $x \in R$, $x \neq 0$ ja x ei ole nullitegur, siis $x \in R^*$.

Olgu $y, z \in R$ ja $y \neq z$. Siis $xy \neq xz$. Tõepoolest, muidu oleks $x(y - z) = 0$, kuid $y - z \neq 0$. S.t. x oleks nullitegur.

Vaatame kujutust $f_x : R \longrightarrow R : y \mapsto xy$.

Me just näitasime, et f_x on injektiivne. Kuna R on lõplik, siis on ta ka sürjektiivne.

$\exists y : f_x(y) = 1$. See y ongi x^{-1}.

Märkus: lõplikkus on oluline. Näiteks ringis $\mathbb{Z}$ nullitegureid ei ole, aga pööratavaid elemente on ainult kaks tükki.

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

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

Teoreemi tõestus. Kui $\gcd(a,n) = 1$, siis leiduvad $u, v \in \mathbb{Z}$ nii, et $ua + vn = 1$ (ringis $\mathbb{Z}$). Ringis $\mathbb{Z}_n$ siis $(u \bmod n)a = ua + vn = 1$.

Kui $\gcd(a,n) = d > 1$, siis $(n/d) \in \mathbb{Z}_n$ ning $a \cdot (n/d) = (a/d) \cdot n = 0$ ringis $\mathbb{Z}_n$. S.t. a on nullitegur.

$\boxed{\textbf{Hulk } \mathbb{Z}_n^*}$

…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

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

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 $xx' \equiv 1 \pmod{m \cdot n}$.

Afiinse šifri murdmine (I)

Ülesanne

Knzilm qlzjw md fjv mgjm mgnf hjf qlxjtfl gl gje utfm gje j qjmg, jwe mglw gl mgdtzgm mgjm klygjkf gl hdtiew'm fjv mgjm, jwe jf gl dklwle gnf pdtmg md fjv fdplmgnwz lifl, Bjwzj finkkle mgl plenxnwl fkddw nw, jwe mglw kjmmle gnp dw mgl qjxb jwe mdie gnp mgjm nm hjf yljiiv rtnml j wnxl mjfml hglw vdt zdm tfle md nm.

Afiinse šifri murdmine (II)

Tekstis esineb täht M 33 korda, tähed J ja L 28 korda. Kolm kõige sagedasemat ingliskeelset tähte on E, T ja A. Vastavus

$$\begin{aligned} \mathrm{E} &\rightarrow \mathrm{M}, \\ \mathrm{T} &\rightarrow \mathrm{J} \end{aligned}$$

annab võrrandisüsteemi

$$\begin{aligned} k \cdot 4 + a &= 12 \mod 26, \\ k \cdot 19 + a &= 9 \mod 26. \end{aligned}$$

Süsteemi lahendiks on $k = 5$, $a = 18$ ja kujutuse

$$x \mapsto 5 \cdot x + 18$$

pöördkujutuseks

$$x \mapsto 21 \cdot x + 12.$$

Afiinse šifri murdmine (III)

Lahendus 1.

`Ozryje kjrtg ex ntl eite eizn dtn kjbtvnj ij its qvne its t ktei, tgs eijg ij eixvrie eite ojwiton ij dxvysg’e ntl eite, tgs tn ij xojgjs izn pxvei ex ntl nxpjeizgr jynj, Htgrt nyzoojs eij pjszbzgj noxxg zg, tgs eijg oteejs izp xg eij ktbh tgs exys izp eite ze dtn wjtyyl fvzej t gzbj etnej dijg lxv rxe vnjs ex ze.`

Afiinse šifri murdmine (IV)

Vastavus

$$\begin{aligned} \text{E} &\rightarrow \text{L}, \\ \text{A} &\rightarrow \text{J} \end{aligned}$$

annab võrrandisüsteemi

$$\begin{aligned} k \cdot 4 + a &= 11 \mod 26, \\ k \cdot 0 + a &= 9 \mod 26 \end{aligned}$$

ja vastavus

$$\begin{aligned} \text{E} &\rightarrow \text{L}, \\ \text{T} &\rightarrow \text{M} \end{aligned}$$

võrrandisüsteemi

$$\begin{aligned} k \cdot 4 + a &= 11 \mod 26, \\ k \cdot 19 + a &= 12 \mod 26. \end{aligned}$$

Afiinse šifri murdmine (V)

Lahendus 2.

Piglet began to say that this was because he had just had a bath, and then he thought that perhaps he wouldn't say that, and as he opened his mouth to say something else, Kanga slipped the medicine spoon in, and then patted him on the back and told him that it was really quite a nice taste when you got used to it.

Ülesanne 2.15

Bmv za sompjx’v epaaf. Vza gona za vnqaj vo epaaf, vza gona za sompjx’v. Za vnqaj Somxvqxi Ezaaf, uzqsz qe eogavqgae k iooj ukc or iavvqxi vo epaaf, kxj, ke vzkv uke xo iooj, za vnqaj somxvqxi Zarrkpmgfe. Kxj vzkv uke uonea. Baskmea adanc Zarrkpmgf vzkv za somxvaj uke gkyqxi evnkqizv ron k fov or Fooz’e zoxac, kxj akvqxi qv kpp.

x	1	3	5	7	9	11	15	17	19	21	23	25
$x^{-1} \pmod{26}$	1	9	21	15	3	19	7	23	11	5	17	25

Ülesanne 2.16

H ejuv krlo mvvw oehwnhwb, jws H ejuv pztv oz j uvid htcziojwo svphlhzw. Oevlv jiv oev xizwb lzio zy mvvl.

Hill's cipher

- Key: a number m and an invertible sqare matrix $M \in \mathbb{Z}_{26}^{m \times m}$.
- Encoding: split the text to sequences of length m. The ciphertext corresponding to $x \in \mathbb{Z}_{26}^{m}$ is $x \cdot M$.
- Decoding: the plaintext corresponding to the ciphertext $y \in \mathbb{Z}_{26}^{m}$ is $y \cdot M^{-1}$.

Example: let $m = 3$ and

$$M = \begin{pmatrix} 15 & 2 & 13 \\ 8 & 21 & 1 \\ 14 & 16 & 7 \end{pmatrix} .$$

Then $\det M \equiv 9 \pmod{26}$, i.e. M is invertible in $\mathbb{Z}_{26}^{3\times 3}$ (because 9 is invertible in $\mathbb{Z}_{26}$).

Let the plaintext be CRYPTOGRAPHY or
$(2, 17, 24), (15, 19, 14), (6, 17, 0), (15, 7, 24)$.

Multiplying all these four vectors with M (from the right) gives us the ciphertext $(8, 17, 3), (1, 3, 0), (18, 5, 17), (19, 15, 6)$ or
IRDBDASFRTPG.

To decode, let us find $M^{-1}\ldots$

$$\left(\begin{array}{rrr|rrr} 15 & 2 & 13 & 1 & 0 & 0 \\ 8 & 21 & 1 & 0 & 1 & 0 \\ 14 & 16 & 7 & 0 & 0 & 1 \end{array}\right) \to \left(\begin{array}{rrr|rrr} 1 & 14 & 13 & 7 & 0 & 0 \\ 8 & 21 & 1 & 0 & 1 & 0 \\ 14 & 16 & 7 & 0 & 0 & 1 \end{array}\right) \to$$

Multiplied the first row with $7 = 15^{-1}$.

$$\left(\begin{array}{rrr|rrr} 1 & 14 & 13 & 7 & 0 & 0 \\ 0 & 13 & 1 & 22 & 1 & 0 \\ 0 & 2 & 7 & 6 & 0 & 1 \end{array}\right) \to \left(\begin{array}{rrr|rrr} 1 & 14 & 13 & 7 & 0 & 0 \\ 0 & 1 & 11 & 12 & 1 & 20 \\ 0 & 2 & 7 & 6 & 0 & 1 \end{array}\right) \to$$

Added the right multiples of the first row to the second and third rows. Then subtracted the sixfold third row from the second.

$$\left(\begin{array}{rrr|rrr} 1 & 14 & 13 & 7 & 0 & 0 \\ 0 & 1 & 11 & 12 & 1 & 20 \\ 0 & 0 & 11 & 8 & 24 & 13 \end{array}\right) \to \left(\begin{array}{rrr|rrr} 1 & 14 & 13 & 7 & 0 & 0 \\ 0 & 1 & 11 & 12 & 1 & 20 \\ 0 & 0 & 1 & 22 & 14 & 13 \end{array}\right) \to$$

Subtracted the twofold second row from the third. Then multiplied the third row with $19 = 11^{-1}$.

$$\left(\begin{array}{ccc|ccc} 1 & 14 & 0 & 7 & 0 & 13 \\ 0 & 1 & 0 & 4 & 3 & 7 \\ 0 & 0 & 1 & 22 & 14 & 13 \end{array}\right) \rightarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 3 & 10 & 19 \\ 0 & 1 & 0 & 4 & 3 & 7 \\ 0 & 0 & 1 & 22 & 14 & 13 \end{array}\right)$$

Added the multiples of the third row to the first and second row. Then added the multiple of the second row to the first row. Hence

$$M^{-1} = \begin{pmatrix} 3 & 10 & 19 \\ 4 & 3 & 7 \\ 22 & 14 & 13 \end{pmatrix}$$

To decode, the vectors making up the ciphertext must be multiplied with M^{-1} from the right.

$(8, 17, 3) \cdot M^{-1} = (2, 17, 24)$, etc.

Types of attacks against encryption systems

- ciphertext-only (*tuntud krüptotekstiga*)
  - Given a ciphertext, find the plaintext and/or the key.
- known-plaintext (*tuntud avatekstiga*)
  - The attacker knows a number of plaintext-ciphertext pairs. With their help, find the key or the plaintext corresponding to some other ciphertext.
- chosen-plaintext (*valitud avatekstiga*)
  - The attacker can invoke the encoding function. Find the key or the plaintext.
- chosen-ciphertext (*valitud krüptotekstiga*)
  - The attacker can invoke the decoding function. Find the key or the plaintext. The decoding function may not be invoked on the ciphertext that we have to decode.

Known-plaintext attack on Hill's cipher

Let m be known (if not, guess). let (x_i, y_i) be the pairs of known plaintext-ciphertext pairs corresponding to an unknown key. I.e. $y_i = x_i \cdot M$.

- Let $x_{i_1}, \ldots, x_{i_m}$ be linearly independent plaintexts.
- Let X be a matrix with the rows $x_{i_1}, \ldots, x_{i_m}$.
- Let Y be the matrix with the rows $y_{i_1}, \ldots, y_{i_m}$.
- $Y = X \cdot M$, hence $M = X^{-1} \cdot Y$.
- If m was unknown then we can use the other plaintext-ciphertext pairs to verify the correctness of M.

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

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

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

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

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

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. $H(\mathbf{X}, \mathbf{Y}) \leq H(\mathbf{X}) + H(\mathbf{Y})$ 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.

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

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

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

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

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

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

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

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

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

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

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

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

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 and the redundancy R_L of L (per letter) 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 ciphertexts. This guarantee vanishes if

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

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.