

Some useful formulas in cryptology.

2006-12-04

Ch. 2:

$$\text{M.R.} = \sum_{i=A}^Z (p_i - \frac{1}{26})^2 = \sum_{i=A}^Z p_i^2 - 0.038$$

$$\text{I.C.} = \frac{\sum_{i=A}^Z f_i(f_i - 1)}{N(N - 1)}$$

Ch. 3:

$$I(X; Y) = H(X) - H(X | Y) = H(Y) - H(Y | X) \geq 0$$

$$H(XY) = H(X) + H(Y | X) = H(Y) + H(X | Y)$$

$$H(X) = - \sum_i f_X(x_i) \log_2 f_X(x_i)$$

$$h(p) = -p \log_2 p - (1 - p) \log_2(1 - p)$$

Redundancy: $D = H_0 - H(M)$

$$H(K | \mathbf{C}) \geq H(K) - ND$$

$$N_0 = H(K)/D$$

Ch. 4:

$$S(D) = \frac{P(D)}{C(D)}$$

$$1(1) \oplus 1(q^L - 1)$$

$$1(1) \oplus \frac{q^L - 1}{T}(T)$$

$$1(1) \oplus \frac{q^{L_1} - 1}{T_1}(T_1) \oplus \dots \oplus \frac{q^{(n-1)L_1}(q^{L_1} - 1)}{T_n}(T_n);$$

$$T_j = p^i T_1, p^{i-1} < j \leq p^i$$

$$S_1 \otimes S_2 \otimes \dots \otimes S_m$$

$$n_1(T_1) \otimes n_2(T_2) = (n_1 n_2 \text{sgd}(T_1, T_2))(\text{mgm}(T_1, T_2))$$

$$\forall m_1, m_2, \dots, m_r \in \mathbb{Z}^+ ; \text{gcd}(m_i, m_j) = 1, i \neq j$$

$$\forall a, u_1, u_2, \dots, u_r \in \mathbb{Z}$$

$$\exists! u \in \mathbb{Z}^+ (a \leq u < a + m) \wedge (u_j = u \pmod{m_j}, 1 \leq j \leq r)$$

where $m = m_1 m_2 \dots m_r$

Ch. 6:

$$n, m \in \mathbb{Z}^+$$

$$\phi(m) = |\{i \in \{1, 2, \dots, m - 1\} \mid \text{gcd}(i, m) = 1\}|$$

$$\forall n; \text{gcd}(n, m) = 1 \quad (n^{\phi(m)} = 1 \pmod{m})$$

Ch. 7:

$$P_D = \max(P_I, P_S)$$

$$P_I = \max_{\mathbf{m}} P(\mathbf{m} \text{ valid})$$

$$P_S = \max_{\mathbf{m}, \mathbf{m}': \mathbf{m} \neq \mathbf{m}'} P(\mathbf{m}' \text{ valid} | \mathbf{m} \text{ valid})$$

Simmons bounds:

$$P_I \geq 2^{-I(\mathbf{M}; E)}$$

$$P_S \geq 2^{-H(E|\mathbf{M})}$$

Ch. 8:

$$a(x) = \sum_{i=1}^k y_i \prod_{1 \leq j \leq k, j \neq i} \frac{x - x_j}{x_i - x_j}$$

The frequency of various letters in English text is given below. Out of 1000 letters the expected number of occurrences for each letter is:

A	73	J	2	S	63
B	9	K	3	T	93
C	30	L	35	U	27
D	44	M	25	V	13
E	130	N	78	W	16
F	28	O	74	X	5
G	16	P	27	Y	19
H	35	Q	3	Z	1
I	74	R	77		

In a text of 80000 letters the most common bigrams and trigrams appear on average as given below:

TH	2161	ED	890	OF	731	THE	1717	TER	232
HE	2053	TE	872	IT	704	AND	483	RES	219
IN	1550	TI	865	AL	681	TIO	384	ERE	212
ER	1436	OR	861	AS	648	ATI	287	CON	206
RE	1280	ST	823	HA	646	FOR	284	TED	187
ON	1232	AR	764	NG	630	THA	255	COM	185
AN	1216	ND	761	CO	606				
EN	1029	TO	756	SE	595				
AT	1019	NT	743	ME	573				
ES	917	IS	741	DE	572				