# Some useful formulas in cryptology.

2013-12-07

**Ch. 1:** CRT: $x \equiv a_1 \pmod{n_1}, \ldots, x \equiv a_k \pmod{n_k}$, $\gcd(n_i, n_j) = 1, i \neq j$.

$$x = \sum_{i=1}^{k} a_i N_i M_i \bmod n,$$

where $N_i = n/n_i$ and $M_i = N_i^{-1} \bmod n_i$.

**Ch. 2:**

$$\begin{aligned} \text{M.R.} &= \sum_{i=A}^{Z} (p_i - \frac{1}{26})^2 = \sum_{i=A}^{Z} p_i^2 - 0.038 \\ \text{I.C.} &= \frac{\sum_{i=A}^{Z} f_i(f_i - 1)}{N(N-1)} \end{aligned}$$

**Ch. 3:**

$$\begin{aligned} I(X;Y) &= H(X) - H(X \mid Y) = H(Y) - H(Y \mid X) \geq 0 \\ H(XY) &= H(X) + H(Y \mid X) = H(Y) + H(X \mid Y) \\ H(X) &= -\sum_i f_X(x_i) \log_2 f_X(x_i) \\ h(p) &= -p \log_2 p - (1-p) \log_2 (1-p) \end{aligned}$$

$$\begin{aligned} \text{Redundancy: } D &= H_0 - H(M) \\ H(K \mid \mathbf{C}) &\geq H(K) - ND \\ N_0 &= H(K)/D \end{aligned}$$

**Ch. 4:**

$$\begin{aligned} S(D) &= \frac{P(D)}{C(D)} \\ 1(1) &\oplus 1(q^L - 1) \\ 1(1) &\oplus \frac{q^L - 1}{T}(T) \\ 1(1) &\oplus \frac{q^{L_1} - 1}{T_1}(T_1) \oplus \cdots \oplus \frac{q^{(n-1)L_1}(q^{L_1} - 1)}{T_n}(T_n); \\ & \quad T_j = p^i T_1, \ p^{i-1} < j \leq p^i \\ S_1 &\otimes S_2 \otimes \cdots \otimes S_m \\ & \quad n_1(T_1) \otimes n_2(T_2) = (n_1 n_2 \gcd(T_1, T_2))(\operatorname{lcm}(T_1, T_2)) \end{aligned}$$

$\forall\, m_1, m_2, \ldots, m_r \in \mathbb{Z}^+ \,; \gcd(m_i, m_j) = 1, \ i \neq j$
$\forall\, a, u_1, u_2, \ldots, u_r \in \mathbb{Z}$
$\exists! u \in \mathbb{Z}^+ \ (a \leq u < a + m) \ \wedge \ (u_j = u \pmod{m_j}, \ 1 \leq j \leq r)$
where $m = m_1 m_2 \cdots m_r$

**Ch. 6:**

$n, m \in \mathbb{Z}^+$
$\phi(m) = |\{i \in \{1, 2, \ldots, m-1\} \mid \gcd(i, m) = 1\}|$
$\forall n; \ \gcd(n, m) = 1 \ \ (n^{\phi(m)} = 1 \pmod{m})$

**Ch. 7:**

$$\begin{aligned} P_D &= \max(P_I, P_S) \\ P_I &= \max_{\mathbf{m}} P(\mathbf{m} \text{ valid}) \\ P_S &= \max_{\mathbf{m},\mathbf{m}':\mathbf{m}\neq\mathbf{m}'} P(\mathbf{m}' \text{ valid}|\mathbf{m} \text{ valid}) \end{aligned}$$

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 occurences 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 | | | | |