# 1 Uwagi:

Jako oznaczenie współrzędnej w $n$-tym wymiarze jest użyta notacja taka jak do ciągów $(m_n)$.
Niezależnie od wyboru wiadomości da się skonstruować $l$ wymiarową hipersferę o takim promieniu $(\sqrt{\sum_{i=0}^{l} m_i^2})$ by punkt $m$ leżał na niej.
Szyfrowanie zadziała jeśli $\exists n(p_{n \bmod k} \neq m_n)$.

# 2 Wyprowadzenie $t$ ze wzoru:

m - punkt leżący na hipersferze

p - punkt przez który i przez $m$ zostanie przeprowadzona prosta, której będą wyliczone wspólnepunkty z hipersferą.

k - liczba wymiarów przestrzeni, w której jest punkt $p$

l - liczba wymiarów hipersfery

$$\sum_{i=0}^{l}(m_i + t(p_{i \bmod k} - m_i))^2 = \sum_{i=0}^{l} m_i^2 \qquad / - \sum_{i=0}^{l} m_i^2$$

$$\sum_{i=0}^{l}(m_i + t(p_{i \bmod k} - m_i))^2 - \sum_{i=0}^{l} m_i^2 = 0$$

$$\sum_{i=0}^{l}(m_i^2 + 2m_i t(p_{i \bmod k} - m_i) + t^2(p_{i \bmod k} - m_i)^2) - \sum_{i=0}^{l} m_i^2 = 0$$

$$\sum_{i=0}^{l}(2m_i t(p_{i \bmod k} - m_i) + t^2(p_{i \bmod k} - m_i)^2) = 0 \qquad / : t$$

$$\sum_{i=0}^{l}(2m_i(p_{i \bmod k} - m_i) + t(p_{i \bmod k} - m_i)^2) = 0 \qquad / - \sum_{i=0}^{l}(2m_i(p_{i \bmod k} - m_i)$$

$$-2\sum_{i=0}^{l} m_i(p_{i \bmod k} - m_i) = t\sum_{i=0}^{l}(p_{i \bmod k} - m_i)^2 \qquad / : \sum_{i=0}^{l}(p_{i \bmod k} - m_i)^2$$

$$t = -2\frac{\sum_{i=0}^{l} m_i(p_{i \bmod k} - m_i)}{\sum_{i=0}^{l}(p_{i \bmod k} - m_i)^2}$$

## 3 Szyfrowanie:

Punkt m w rezultacie długości promienia leży na hipersferze. By uniknąć niecałkowitego wyniku wynikiem są dwa ciągi - reszty z dzielenia i podłogi ilorazów
Do reszt z dzielenia dodawane jest $p_{n \bmod k} \bmod k$ na wypadek, gdy $a_n = 0$ i by zamaskować promień hipersfery.
Wejście:

m - wiadmość

p - klucz

k - długość klucza

l - indeks ostatniego elementu wiadomości

Wyjście:

r - reszty z dzielenia wyrazów $e$ przez $b$

q - podłogi wyników dzielenia wyrazów $e$ przez $b$

b - mianownik do użycia przy odszyfrowywaniu

$a_n = p_{n \bmod k} - m_n$
$b = \sum\limits_{i=0}^{l} a_i^2$
$c = 2\sum\limits_{i=0}^{l} m_i a_i$
$e_n = bm_n - a_n c$
$r_n = e_n \bmod b + (p_{n \bmod k} \bmod k)$
$q_n = \lfloor \frac{e_n}{b} \rfloor$

## 4 Odszyfrowywanie:

Punkt $m$ w rezultacie długości promienia leży na hipersferze, a $\frac{e_n}{b}$ jest punktem wspólnym prostej i hipersfery, więc też leży na hipersferze.
Wejście:

r - reszty z dzielenia wyrazów $e$ przez $b$

q - podłogi wyników dzielenia wyrazów $e$ przez $b$

b - mianownik do użycia przy odszyfrowywaniu

p - klucz

k - długość klucza

l - indeks ostatniego elementu zaszyfrowanej wiadomości

Wyjście:

m - wiadmość

$e_n = bq_n + r_n - (p_{n \bmod k} \bmod k)$
$f_n = bp_{n \bmod k} - e_n$
$g = \sum_{i=0}^{l} f_i^2$
$h = 2\sum_{i=0}^{l} e_i f_i$
$d = gb$
$m_n = \frac{ge_n - f_n h}{d}$