# XOR

Za toto jsem dostal zápočet na IPS I., tak nevím, jak moc se to sem hodí. Zprávu $N$ zašifrujeme do čísla $Z$ o základu 2 (triviálně umíme skoro vždy). Pro každou $k$-tici generálů $G_i$ uděláme následovné:

1. každý generál $l$ dostane náhodné binární číslo $g_i^l$ délky $|Z|$
2. číslo $Z_i = Z \oplus g_i^1 \oplus g_i^2 \oplus \ldots \oplus g_i^k$ zveřejníme
3. zveřejníme všech seznam generálů ve všech $\binom{n}{k}$ skupinách

Pak zřejmě:

1. pokud se sejde nějaká $k$-tice $G_i$, pak mají k dispozici čísla $Z_i, g_i^1, g_i^2, \ldots, g_i^k$
2. zprávu $Z$ dekonstruují jako $Z = Z_i \oplus g_i^1 \oplus g_i^2 \oplus \ldots \oplus g_i^k$
3. stačí již dešifrovat zprávu $Z$ do původní $N$

Kritická část je šifrování pomocí $XOR$, ale:

$$Z_i = Z \oplus g_i^1 \oplus g_i^2 \oplus \ldots \oplus g_i^k = Z \oplus Q_k$$
$$Z_i \oplus Q_k = Z \oplus Q_k \oplus Q_k = Z \oplus 0 = Z$$

Nevýhodou je, že musíme vygenerovat $\binom{n}{k} \cdot k \cdot |Z|$ bitů a ty rozdistribuovat. Pokud se to však podaří, pak neprozradíme ani jeden bit informace v procesu (*not a bit*), neboť $XOR$ náhodným číslem je opět náhodné číslo..

# Algebraický přístup

Předchozí řešení je dost technické. Úloha lze snad řešit i víc matematicky. Předpokládáme, že zprávu $N$ zašifrujeme do $k$-dimenzionálního prostoru (např. rozdělíme na $n$ částí). Pak vygenerujeme $n$ různých nadrovin, které procházejí tímto bodem a jejich parametry rozdáme generálům. Jestliže se jich sejde alespoň $k$, tak jejich nadroviny jednoznačně určí původní $N$ (méně určí nadrovinu o dimenzi nižší, což však nestačí).
Nevýhodou je, že předpokládáme zašifrovatelnost do bodu v nějakém prostoru. To je mnohem silnější předpoklad než u $XOR$ řešení. Pokud však můžeme o $N$ něco předpokládat, tak $k-1$ generálů má nadrovinu o jedna nižší dimenzi, kde se zpráva nachází, což může být problém.
Druhé řešení se mi líbí v tom, že každý generál dostane pouze jednu sadu parametrů, nikoliv pro každou možnou skupinu.