Algebry a šifry

Úloha 1: Dešifrujte zprávu zašifrovanou Caesarovou šifrou s posunem $k = 3$.

```
KHOOR ZRUOG
```

Vzorec pro dešifrování: $m = (c - k) \bmod 26$.

Úloha 2: Vypočtěte následující výrazy.

1. $7^4 \equiv ? \bmod 13$
2. $7^{12} \equiv ? \bmod 13$

Čemu se rovná $\varphi(13)$? Proč?

Úloha 3: Ověřte Eulerovu větu pro $n = 7$ a $m = 3$, tj. že $m^{\varphi(n)} \equiv 1 \bmod n$.

Doplňte tabulku mocnin čísla 3 modulo 7:

3^1	3^2	3^3	3^4	3^5	3^6	3^7

Kdy se poprvé vrátíte na 1? Odpovídá to hodnotě $\varphi(7)$?

Úloha 4: Alice a Bob provádějí DHKE s veřejnými parametry $p = 23$ a $g = 5$. Alice si zvolí tajné číslo $a = 6$, Bob si zvolí tajné číslo $b = 15$.

1. Vypočtěte, co Alice pošle Bobovi: $A = g^a \bmod p = 5^6 \bmod 23$
2. Vypočtěte, co Bob pošle Alici: $B = g^b \bmod p = 5^{15} \bmod 23$
3. Alice spočte sdílené tajemství: $k = B^a \bmod p$
4. Bob spočte sdílené tajemství: $k = A^b \bmod p$
5. Ověřte, že oba dostali stejný výsledek.

Eva vidí jen $g = 5$, $p = 23$, A a B. Zkuste z těchto hodnot zjistit a nebo b.

Úloha 5: Vyřešte rovnici

$$5^x \equiv 8 \bmod 23$$

tj. najděte x takové, aby platila rovnost.

Jak dlouho by tento postup trval pro $p \sim 2^{2048}$?

Užitečné vzorečky

- **Caesarova šifra:** šifrování $c = (m + k) \bmod 26$, dešifrování $m = (c - k) \bmod 26$
- **XOR (OTP):** $c = m \oplus k$, dešifrování $m = c \oplus k$; platí $a \oplus a = 0$
- **Eulerova funkce:** $\varphi(p) = p - 1$ pro prvočíslo p; $\varphi(pq) = (p-1)(q-1)$
- **Eulerova věta:** pro $\gcd(m, n) = 1$ platí $m^{\varphi(n)} \equiv 1 \bmod n$
- **Malá Fermatova věta:** pro prvočíslo p a $m \in \mathbb{Z}_p^*$ platí $m^{p-1} \equiv 1 \bmod p$
- **DHKE:** sdílené tajemství $k = g^{ab} \bmod p = B^a \bmod p = A^b \bmod p$