

# Matteklubben

## Vårterminen 2015, lektion 7

### Krypto

Beräkna följande uttryck.

1.  $*5 + *8$
2.  $*95 + *28$
3.  $*6 \cdot *6$
4.  $*50 \cdot *79$
5.  $*83 \cdot *01$

Lös följande ekvationer. Ange *alla* lösningar (två lösningar räknas som samma om de motsvarar samma \*-tal).

6.  $*x + *8 = *4$
7.  $*x \cdot *7 = *4$
8.  $*x \cdot *2 = *0$
9.  $*yx \cdot *50 = *50$
10.  $*yx \cdot *01 = *83$



11.  $*x \cdot *7 = *1$

12.  $*yx \cdot *67 = *01$

13.  $*zyx \cdot *267 = *001$

Lös följande uppgift genom att utnyttja dina tidigare resultat på ett smart sätt!

14.  $*yx \cdot *67 \cdot *03 = *43$

Alice vill skicka hemliga meddelanden till Bob. De har var sin kopia av en tabell som identifierar bokstäver och symboler med \*-tal. När Alice skickar meddelanden så kodar hon varje bokstav genom att multiplicera bokstaven med \*67 och skickar resultatet till Bob. Exempelvis om hon ska skicka bokstaven X så räknar hon  $X \cdot *67$ :

$$X \cdot *67 = *87 \cdot *67 = *29 = A.$$

Resultatet blev A. Det betyder att hon ersätter X med A och skickar bokstaven A till Bob. Bob vet att Alice kodar varje bokstav genom att multiplicera bokstaven med \*67. Hur ska han göra för att enkelt avkoda bokstaven?

15. Hämta ett krypterat meddelande som Alice skickat och dekryptera det!

### Att fundera på

Alice och Bob använde alltså en tabell och en hemlig nyckel (nyckeln var \*67) för att skicka krypterade meddelanden. Skulle någon obehörig få tag på tabellen så känner hen ändå inte till deras hemliga nyckel vilket gör det svårt att läsa meddelandena. För att göra kryptot ännu säkrare kan de bestämma att de byter nyckel regelbundet efter något bestämt system som bara de känner till. Ju oftare de byter nyckel och ju krångligare system de har för att byta nyckel ju svårare blir det för någon obehörig att läsa deras meddelanden!

Men vilka \*-tal kan de använda som nyckel? Fungerar det med vilket \*-tal som helst?

Tabellen innehåller bara vissa \*-tal. Finns det någon särskild anledning till att de har valt just de talen? Hade de kunnat haft en större tabell med alla \*-tal mellan \*00 och \*99?