Universiteit van Stellenbosch
Toegepaste Wiskunde 314

Tutoriaal 11: Donderdag 11 Mei 2017

1. **Die RSA kripto-sisteem met blok lengte protokol 2 syfers.**

   (a) Gebruiker A het sleutels $p = 11$, $q = 13$ and $d = 37$ gekies. Bepaal n en e.

   (b) Jy wil die boodskap YES (25 05 19) aan A stuur. Hoe enkripteer jy?

   (c) Gebruiker A ontvang (27, 119). Hoe dekripteer A?

2. **Die ElGamal kripto-sisteem met blok lengte protokol 2 syfers.**

   (a) User Gebruiker A het sleutels $n = 97$, $\alpha = 40$ en $a = 30$ gekies. Bepaal β.

   (b) Jy wil die boodskap JA (10 01) aan A stuur. Hoe enkripteer jy?
   (Gebruik masker $k = 7$ vir beide blokke).

   (c) Gebruiker A ontvang (92, 39), (91, 92), (51, 59). Hoe dekripteer A?

University of Stellenbosch
Applied Mathematics 314

Tutorial 11: Thursday 11 May 2017

1. **The RSA cipher with block length protocol 2 digits.**

   (a) User A has chosen keys $p = 11$, $q = 13$ and $d = 37$. Determine n and e.

   (b) You need to send the message YES (25 05 19) to user A. How do you encrypt?

   (c) User A receives (27, 119). How does A decrypt?

2. **The ElGamal cipher with block length protocol 2 digits.**

   (a) User A has chosen keys $n = 97$, $\alpha = 40$ and $a = 30$. Determine β.

   (b) You need to send the message JA (10 01) to user A. How do you encrypt?
   (Use mask $k = 7$ for both blocks).

   (c) User A receives (92, 39), (91, 92), (51, 59). How does A decrypt?