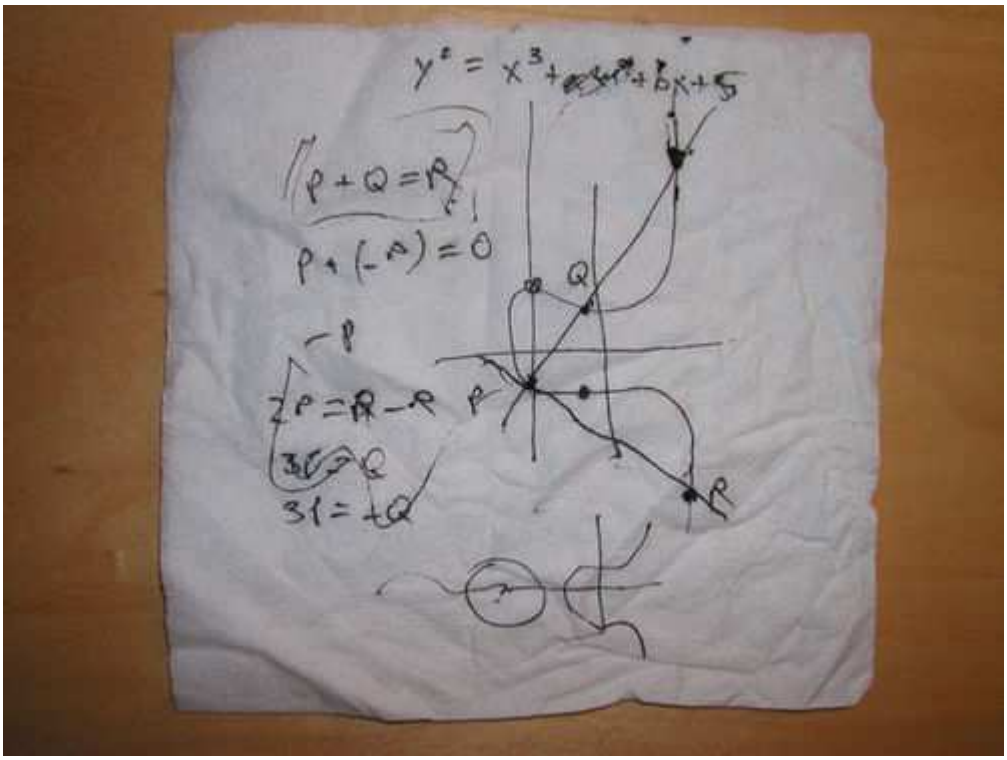
Doc. RNDr. Miroslav Kureš, Ph.D.

Kryptografie s veřejným klíčem

Alice chce poslat po internetu zašifrovanou zprávu Bobovi, ale nemůže mu předem poslat klíč. Řešením je užít klíče dva: jeden pro šifrování (veřejný), druhý pro dešifrování (tajný). To lze realizovat za pomoci tzv. jednosměrných funkcí. Seznámíme se s nejrozšířenějším systémem RSA, se systémem ECC využívajícím magické eliptické křivky a s aktuálními novinkami.



14. 11. 2012 v 19h

sál Moravské zemské knihovny, Kounicova 65a, Brno, vstup volný

Přednáška se koná v rámci Týdne vědy a techniky, motto: *„Energie vědy“*.
Energie je všude kolem nás. Hvězdy i planety, příliv i vítr, lidské bytosti i jednobuněčné organismy, nanočástice i atomy, vše je plné energie. Energie rozděluje i spojuje, energie je nezbytná k životu. Energie je také síla, vůle k činům. Poznejte energii ve vědě na Týdnu vědy a techniky.