UNIWERSYTET SZCZECIŃSKI
WYDZIAŁ MATEMATYCZNO-FIZYCZNY

WYDZIAŁ MATEMATYCZNO – FIZYCZNY
Instytut Matematyki

Zaprasza na wykład pod tytułem:

Prime numbers and elliptic curves in cryptology - selected topics

który wygłosi:

prof. Jacek Pomykała

Uniwersytet Warszawski

ABSTRACT:

In the lecture we discuss the role of prime and almost prime numbers in designing the classical cryptographic systems as well as the cryptosystems based on elliptic curves. We will focus on some important theoretical problems closely related to efficiency and security of the familiar cryptosystems. This includes the problem of an upper bound for the least Dirichlet character nonresidue and the analogous problem for elliptic curves. We will give some applications to cryptology like factoring integers with oracles or reductions between hard computational problems.

Wykład odbędzie się **26 września 2018 r.** (środa)
o godz. **14.00** w sali 212
w budynku Wydziału Matematyczno – Fizycznego.