

Tardes no CMUP

26 de Maio de 2006

Anfiteatro 0.05

14:30-15:20 Gabriela Gomes
(Inst.Gulbenkian da Ciência)

**Epidemiological consequences of imperfect
immunity**

Café na sala de convívio do DMP

15:45-16:35 António Machiavelo (DMP) e
Rogério Reis (DCC)

"Há casos jurídicos que são como as cerejas..."
(Crónica de um ataque a uma cifra ingénua)

Tardes no CMUP 26 de Maio de 2006

Resumos

Epidemiological consequences of imperfect immunity

The *SIR* (susceptible-infectious-resistant) and *SIS* (susceptible-infectious-susceptible) frameworks for infectious disease have been extensively studied and successfully applied. They implicitly assume the upper and lower limits of the range of possibilities for host immune response. However, the majority of infections do not fall into either of these extreme categories. Our research group is generally concerned with the construction and analysis of mathematical formalisms that straddle this range of imperfect immunity.

The specific problem addressed in this talk is one by which pathogens mutate and often recombine, generating a rich pool of antigenic types. The pressures of transmission and host immunity restrict diversity. Selection occurs and pathogen population structure emerges as to best escape host immunity. Pathogen population structure and evolution must be related to the epidemic dynamics of the disease. But how? What can we say about control? How do interventions affect pathogen population structure, and what are the consequences for epidemic dynamics? While computational models are beginning to address these challenges, there is a desperate need for new analytical tools, new ideas and new talents.

"Há casos jurídicos que são como as cerejas..." (Crónica de um ataque a uma cifra ingénua)

Com o advento dos computadores digitais, depois da Segunda Guerra Mundial, a criptografia de "papel e lápis" ficou essencialmente relegada para os clubes de amadores de criptogramas, apesar de ter ainda sido usada pelos serviços de espionagem, até ao final da década de 80. Os computadores permitem automatizar processos, cuja morosidade e complexidade desencorajariam o mais temerário dos espões a comunicar fosse o que fosse com a base. Apesar disto, para muitas cifras "tipográficas", apesar de não serem hoje consideradas seguras, não são conhecidos métodos de ataque que não necessitem da ajuda de um pedaço de texto, que se "adivinha" estar presente na mensagem, para que possam funcionar. A "Bifid", uma das cifras criadas pelo misterioso Delastelle (1840-1902) é um destes casos. Apesar de não se lhe conhecer utilização "séria", é uma das mais populares cifras entre os "amadores" e reputadamente uma das mais "difíceis". O que iremos apresentar é um método de quebra para esta cifra, que para além de não necessitar de acesso a uma parte do texto original pode ser automatizado por um programa que funciona em tempo útil.