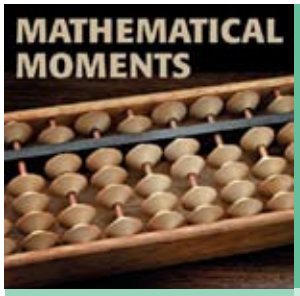
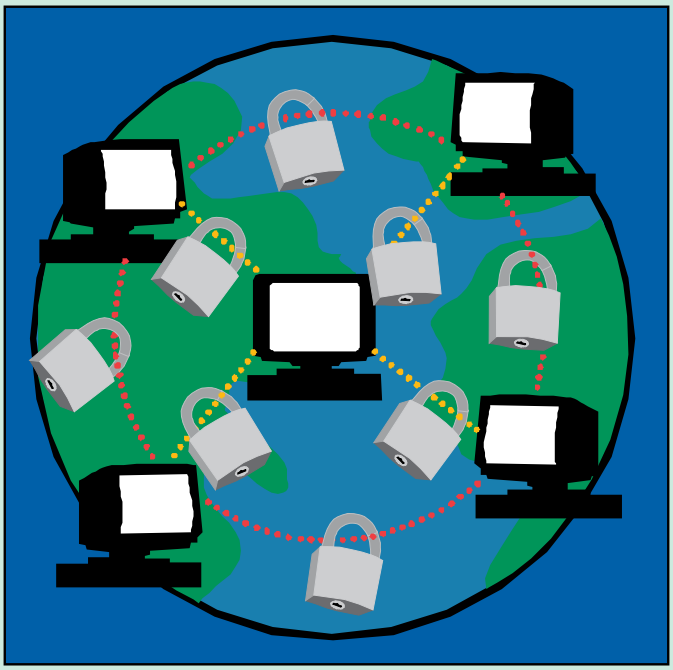


Zabezpieczanie komunikacji internetowej

Nikt nie mógłby robić zakupów, opłacać rachunków czy też prowadzić interesów, bezpiecznie korzystając z internetu, bez matematyki szyfrowania. Dzisiejsze zaawansowane techniki szyfrowania, chociaż oparte na faktach algebraicznych udowodnionych wieki temu, zostały opracowane w ciągu ostatnich dwudziestu pięciu lat.

Szyfrowanie przy pomocy klucza publicznego pozwala użytkownikowi opublikować klucz szyfrujący, do użytku przez wszystkich, i zachować w tajemnicy klucz deszyfrujący. Jeden z takich algorytmów, zwany RSA, używany jest do szyfrowania w nowoczesnych przeglądarkach. Narodowy Instytut Standardów i Technologii (w USA) przyjął ostatnio Zaawansowany Standard Szyfrowania (Advanced Encryption Standard), który zostanie zastosowany w komunikacji elektronicznej w niedalekiej przyszłości. Nowy standard wykorzystuje permutacje, arytmetykę modularną, wielomiany, macierze oraz ciała skończone do swobodnego ale zarazem bezpiecznego przesyłania informacji.



Więcej informacji:
"Communications Security for the Twenty-first Century", Susan Landau, *Notices of the American Mathematical Society,* April 2000.

Translation by Agnieszka Dardzińska-Głębocka, Politechnika Białostocka, courtesy of the Polskie Towarzystwo Matematyczne

AMS
American Mathematical Society

*Program **Mathematical Moments** promuje znaczenie i rozumienie roli, jaką matematyka odgrywa w nauce, przyrodzie, technice i kulturze.*

www.ams.org/mathmoments