

Crypto moderne

HOW TO USE PGP TO VERIFY
THAT AN EMAIL IS AUTHENTIC:

LOOK FOR THIS
TEXT AT THE TOP.



IF IT'S THERE, THE EMAIL IS PROBABLY FINE.

Cryptographie Moderne

Hypothèses de calcul classique

- Factorisation entière (retrouver p, q étant donné $N = pq$)
 - RSA
- Logarithme discret (retrouver x étant donné $y = g^x$)
 - Diffie-Hellman (Corps finis ou Courbes elliptiques)
 - El Gamal
 - DSA