Conclusion

- La version présentée (appelée “textbook” RSA) n’est pas sûre
  - Beaucoup de détails passés sous le tapis nécessaire à la sécurité
  - Optimisations non mentionnées pour rendre le schéma plus performant en pratique
- Le chiffrement asymétrique moderne est souvent basé sur la méthode de Diffie-Hellman implémenté sur les courbes elliptiques
- Dans TLS, RSA est utilisé pour la signature de certificat et l’échange de clé symétrique
- OpenSSH supporte les clé RSA pour l’authentification et l’échange de clé symétrique
  - Était le protocole par défaut jusqu’à la version 9.5 (2023-10-04)

Références

Si vous aimez lire des vieux articles

- DIFFIE, W., & HELLMAN, M. E. (1976). **New Directions in Cryptography**. IEEE TRANSACTIONS ON INFORMATION THEORY, 22(6).
- Rivest, R. L., Shamir, A., & Adleman, L. (1978). **A method for obtaining digital signatures and public-key cryptosystems**. Communications of the ACM, 21(2), 120-126.
- Rivest, R. L., Adleman, L., & Dertouzos, M. L. (1978). **On data banks and privacy homomorphisms**. Foundations of secure computation, 4(11), 169-180.