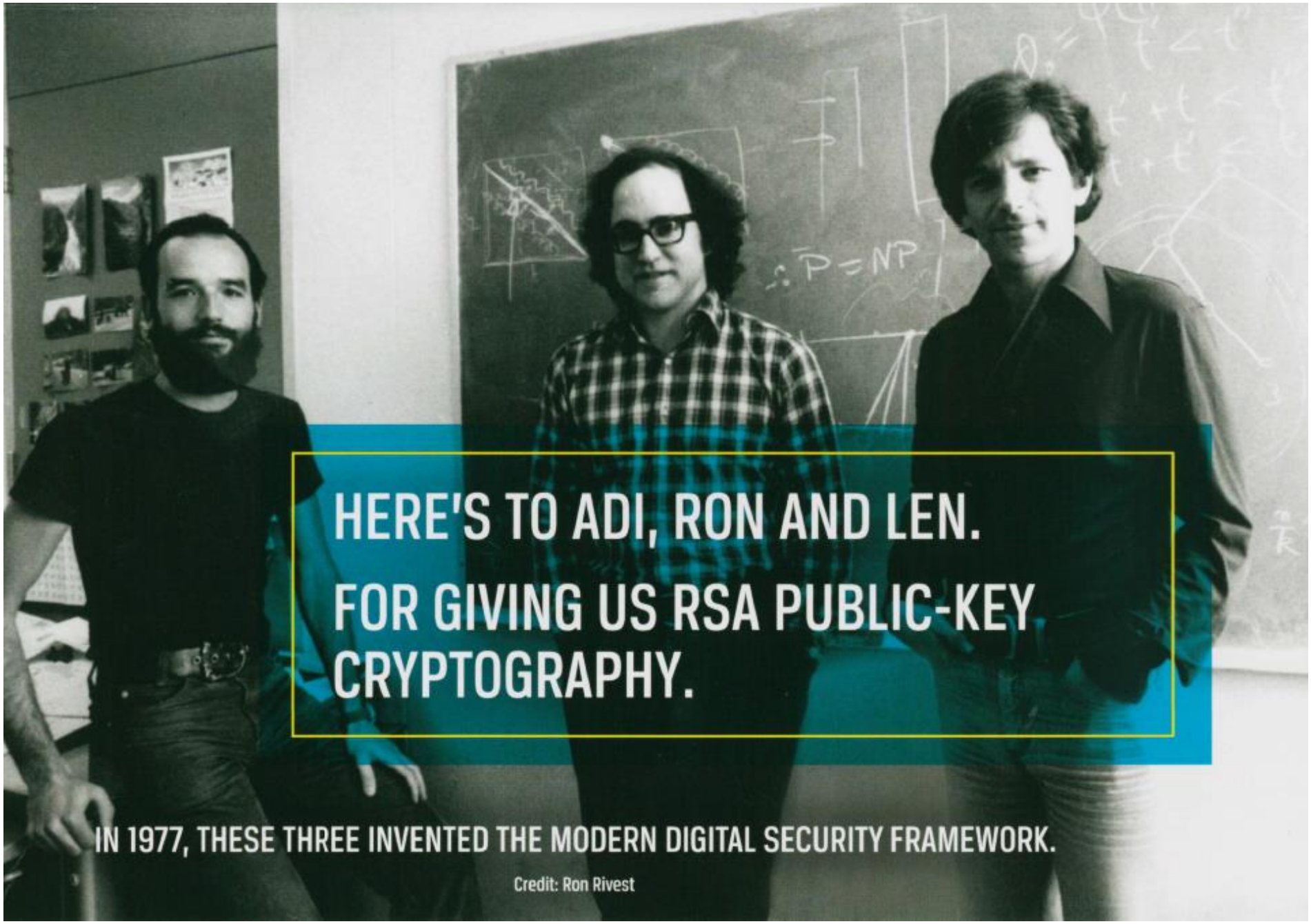
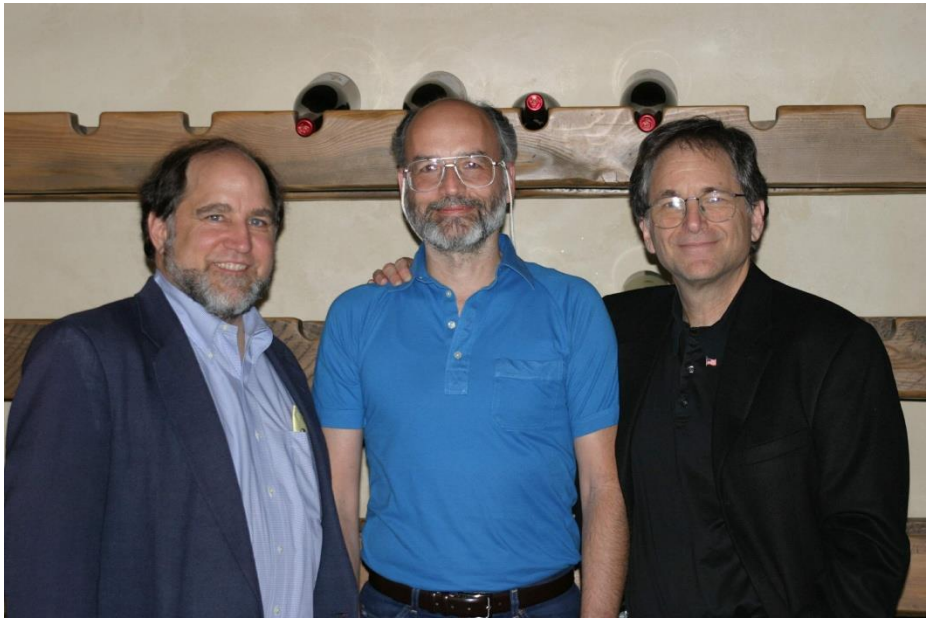

HERE'S TO ADI, RON AND LEN.
FOR GIVING US RSA PUBLIC-KEY CRYPTOGRAPHY.
IN 1977, THESE THREE INVENTED THE MODERN DIGITAL SECURITY FRAMEWORK.
Credit: Ron Rivest

RSA

- Diffie-Hellman consente di condividere un segreto, ma non permette di criptare un messaggio o di firmare digitalmente un documento.
- La prima e diffusa soluzione per realizzare questi compiti è il crittosistema RSA, introdotto da Ronald Rivest, Adi Shamir e Leonard Adleman nel 1977.



R. Rivest, A. Shamir, L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”, Communications of the ACM. 21 (2): 120–126, February 1978.

RSA – key generation

- RSA si basa sulla difficoltà di fattorizzare grandi numeri interi.

- Bob sceglie due primi grandi e diversi p e q e li moltiplica ottenendo il **modulo pubblico**:

$$n = pq$$

- Conoscendo p e q, Bob può calcolare $\varphi(n) = (p - 1)(q - 1)$ e:
  - sceglie randomicamente l'**esponente di cifratura** e tale che

$$\text{GCD}(e, (p - 1)(q - 1)) = 1$$

  - calcola **l'esponente** d tale che

$$de \equiv 1 \pmod{(p - 1)(q - 1)}$$

- Bob's **private key**: (p, q, d)
- Bob's **public key**: (n, e)

RSA – cifratura

- Alice scrive il messaggio segreto come numero m.
- Se m è più grande di n, si spacchetta il messaggio in blocchi, ognuno corrispondente a un numero $< n$.
- Alice calcola: $c \equiv m^e \pmod{n}$ e manda c a Bob come il ciphertext corrispondente a m

RSA - decifratura

- Per il teorema di Eulero, se GCD(a, n) = 1, allora $a^{\varphi(n)} \equiv 1 \pmod{n}$.
- Nel nostro caso, $\varphi(n) = \varphi(pq) = (p-1)(q-1)$.
- Supponiamo che GCD(m, n) = 1.
- Essendo $de \equiv 1 \pmod{\varphi(n)} \rightarrow de = 1 + k\varphi(n)$, essendo k intero.
- Bob può decifrare c calcolando $m \equiv c^d \pmod{n}$, infatti:

$$c^d \equiv \left(m^e\right)^d \equiv m^{1+k\varphi(n)} \equiv m \cdot \left(m^{\varphi(n)}\right)^k \equiv m \cdot (1)^k \equiv m \pmod{n}$$

Scelta di Bob

- Bob sceglie p e q come due primi grandi, indipendenti l'uno dall'altro.
- Il valore di p e q sono molto grandi: almeno 100 cifre.
- Sarebbe preferibile sceglierli con lunghezza leggermente diversa.