THEOREM OF THE DAY

Bézout's Identity *Let a and b be positive integers with greatest common divisor equal to d. Then there are integers u and v such that $au + bv = d$.*

Angela's public key, using secret key $K = 99$:

$p = 109$

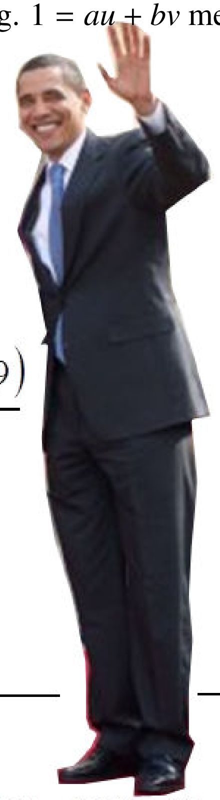
$r = 6$

$y = 68 = r^K \bmod p = 6^{99} \bmod 109$

Barack encrypts his message, $m = 66$, using secret key $L = 55$:

$$s = 103 = r^L \bmod p = 6^{55} \bmod 109$$

$$\begin{aligned} c = 2706 &= 66 \times 41 = m \times x \\ &= m \times (y^L \bmod p) \\ &= 66 \times (68^{55} \bmod 109) \end{aligned}$$



Angela finds x:

$$\begin{aligned} x &= y^L \bmod p \\ &= (r^K)^L \bmod p \\ &= (r^L)^K \bmod p \\ &= s^K \bmod p = 103^{99} \bmod 109 = 41 \end{aligned}$$

Angela finds x^{-1}...

$$\begin{aligned} 109 &= 41 \times 2 + 27 \\ 41 &= 27 \times 1 + 14 \\ 27 &= 14 \times 1 + 13 \\ 14 &= 13 \times 1 + 1 \end{aligned}$$

$$\begin{aligned} 1 &= 41 - (109 - 41 \times 2) - ((109 - 41 \times 2) - (41 - (109 - 41 \times 2))) \\ 1 &= 41 - 27 - (27 - (41 - 27)) \\ 1 &= 14 - (27 - 14) \\ 1 &= 14 - 13 \end{aligned}$$

$$1 = 8 \times 41 + -3 \times 109$$

$$8 \times 41 = 1 \bmod 109$$

$$8 = 41^{-1} \bmod 109 = x^{-1}$$

... and hence finds: $m = c \times x^{-1} = 2706 \times 8 = 21648 = 66 \pmod{109}$

Euclid's greatest common divisor algorithm produces a constructive proof of this identity since values for u and v may be established by substituting backwards through the steps of the algorithm. This is illustrated for the values $a = 109$ and $b = 41$, with greatest common divisor $d = 1$, in the final box, below left, of our illustration. We find that $u = -3$ and $v = 8$ satisfy the identity. Our Angela–Barack story is based on the corollary of Bézout that we may efficiently invert a modulo b, or b modulo a: e.g. $1 = au + bv$ means that $au = 1 \pmod b$ whence $a^{-1} = u \pmod b$.

So we may efficiently reverse a multiplication in modular arithmetic. By contrast, there is no known method for efficiently reversing an exponentiation. If I give you the result of the calculation $r^K \bmod p$, say, and tell you the values of r and p, then in general an exhaustive search will be required to recover the value of K. This is called the *discrete logarithm problem* in analogy with the real number logarithm: the power of the base which gives the argument. For numbers with hundreds of digits a modular exponent may be calculated in milliseconds; a discrete logarithm will in general require millennia!

Whence the famous and widely-used ElGamal encryption algorithm: Angela publishes a three-part *public key* (p, r, y) based on a private key K; Barack uses Angela's public key to encrypt message m as the pair (s, c), where c is m multiplied by x. By a trick of modular arithmetic, Angela may use s, c and K to recover x and, thereafter, Bézout's identity to recover m. Without solving the discrete logarithm problem no third party may realistically hope to discover x (except, of course, by compromising Angela's or Barack's individual security protocols).

Bézout's name attaches to this identity, first presented by Claude-Gaspard Bachet de Méziriac in 1624, thanks to his publication, in 1779, of its generalisation to polynomials. The ElGamal encryption algorithm is named after Taher Elgamal who published it in 1985.

Web link: www.di-mgt.com.au/crypto.html: an excellent source on cryptography: click on Euclidean algorithm and public key cryptography using discrete logarithms.

Merkel and Obama images: www.whitehouse.gov/blog/2009/04/03/a-town-hall-strasbourg

Further reading: *Everyday Cryptography: Fundamental Principles and Applications* by Keith M. Martin, Oxford University Press, 2012.