The repeated squaring alg.

Input: g in G and x>0 ; **Output**: g^x

write $x = (x_n\ x_{n-1} \ldots x_2\ x_1\ x_0)_2$

$y \leftarrow g$, $z \leftarrow 1$

for i = 0 to n do:

    if (x[i] == 1): $z \leftarrow z \cdot y$

    $y \leftarrow y^2$

output z

example: g^{53}

y	z
g^2	g
g^4	g
g^8	g^5
g^{16}	g^5
g^{32}	g^{21}
g^{64}	$\mathbf{g^{53}}$