12) a) By Lecture and Fermat's Little Th. the order must divide $p-1$, in this case $p-1=2^{16}$ so possible orders are $2, 4, 8, 16, \ldots, 2^{16}$

b) We have shown this in class

c) The orders 2, 4, etc:

$13, 13^2 \equiv 169, 13^4 \equiv 169^2 \equiv 28561 \pmod{p}$,

$13^8 \equiv 57219$, $13^{16} \equiv 47589$, ...

$13^{4096} \equiv 65536 \neq 1$, $13^{8192} \equiv 1 \Rightarrow$ Order is 8192

13) If $\text{OrderMod}_p(g) = p-1$ then g is prim. root. For g not to be prim. root the order must be smaller and thus a proper divisor.

b) Assume g is not a prim. root. Then $e = \text{OrderMod}_p(a)$ is proper divisor of $p-1$. Let q be a prime divisor of $\frac{(p-1)}{e}$. Then $e \mid \frac{p-1}{q}$ and thus $g^{\left(\frac{p-1}{q}\right)} \equiv 1 \pmod{p}$.

c) Calculation shows that neither of these 3 numbers is $\equiv 1$, so by b) 11 must be a primitive root modulo 1009.

[5] a) $26+26+10 = 62$ symbols. $\Rightarrow 62^4 =$ 14776336 sequences. ~ count bad sequences:

b) Sequences w/o upper case: 36^4, w/o digits: 52^4 (lower)

Inclusion/exclusion: seqs. w/o upper or lower case or digit: $36^4 + 36^4 + 52^4 - \underline{26^4} - \underline{26^4} - \underline{10^4}$

were double counted. {only upper / only lower / only digits}

$= 9746896$ bad ones, so 5029440 sequences fulfilling all conditions.

c) The policy eliminates "dummy" PW. (such as 1234), but at the price of making a brute force search almost 3 times easier! Not a good policy!

14] $2^{50}/10^{10} \approx 113000$, ≈ 31.27 hours (already short time...), so 15.6 hours for half the keys.
Since 6 years $\hat{=}$ factor 10, use $\log_{10}(15.6) = 1.19$
so after 1.19 units of 6 years, so after
$6 * 1.19 = 7.15$ years, rounded up to
8 years. (For the full set of keys one gets
$6 * \log_{10}(31.27) \approx 9$ years