1.
running john shadow.txt (which containing the given hashes) results in:
carol:carol84
alice:1234
john:dmsh
bob:w4lt0n
kelly:7cV1h
norman:M4s,b9
running john with rockyou wordlist:
eve:wertyuio
running john with filmnames
dave:SinCity

running hashcat -a 3 -m 1500 shadow
also gives some passworts. hashcat calculating the hashes on gpu, so its significantly faster then john uses cpu.

advanced wordlists attacks with different rules are not revealing new passwords.

2. Das gegebene Schema ist nicht sicher. Wenn ich nur eine Stelle des Passwords kenne kann ich das komplette Passwort errechnen.

Außerdem ist XOR eine sehr günstige Operation. Deshalb kann es auch noch schnell errechnet werden.

3.

methode	vorteil	nachteil
random number	nicht vorhersagbar	not unique
timestamp	unique	vorhersagbar
counter	unique	vorhersagbar