

8INF857 - Sécurité informatique - Devoir 1 « Les mots de passe »
Bondue Emeric, Lecoq Simon

Question 1

Login	Hash - sha256(Password)	Password
Jamie	527aa9f431539da8e151d5434d1d5e611d973f601d8e970790882624554146b0	runner
Cerceii	a92f6bdb75789bcccc118adfcf704029aa58063c604bab4fcdd9cd126ef9b69af	mustang
Jon	dfb2b4b12b7d9d541e0b99dea14d563ca64a560547f2516ec6c88d2efc739a9e	bisou
Briene	9ce8db922a8f4a7abd859adee70bd8b7a63321265487da54cf4bed6a69eb3e1b	jennifer
Ramsey	91246e60ed7dc0330ab443434feba9e5aec9a0f2de5dec0f7575fd2a3caaa421	nascar
Joffrey	7b85175b455060e3237e925f023053ca9515e8682a83c8b09911c724a1f8b75f	carlos
Sansa	dc9f28b12dd1818ee42fffc92ecb940386214598837348d30d3c6c0b7b57e34c9	fire
Bran	548a39619a812e451be4ec19229bafffbab2cccf539c8b1e430de93edd25716	debbie
Rickon	d7910c6961a5ed626fd309d40e40c40566f4aa05b1fb54a856a0bab84f546c6f	partie
Arya	47798d12ae31ce5a6d9c9dddec7bc9f2a27fffa424b7f2a154fa0e26690972de	billy

Question 2

Login	Salt - sha256(Login)	Hash - sha256(Password . Salt)
Jamie	e7a4477ec945697c1003e467ec7b8fc2c485d90453882a203c08956d377d8cbd	eb1ca7f22860c8ee6f23b019c99a00374dbfc98523573f34cf3b68e3562d40d3
Cerceii	2626d6426194ffd0e6799204ec2e01c22e372f6f37f12d293f8233fe51d3b6a6	d1029f6b1d5a3d169a9efcf466068cb21ac60b887b4cc3a9aa5e20ec69fbdadbd
Jon	bb472edb86809a761936d90c70aeb4346618aa71da7a00c16e334863499108fd	d74663c0f5e7530efa0c94cf54f548a2067b83a236e4e60a0fb0a2c6beced0f8
Briene	1c0829aa780710fb35d4c774682507350f85b0a05111ba24d54fff7db3a4e73d	47248e85f9a8889ba0532b4ed1399101897f6df6f23add4512802dcbb3ba35b0
Ramsey	2916fa2bb61281073571eed18305bf569eca21466084a335587f4405ba98a94e	04da7f89917a64176ec3a4e41377c1467a0f01304a3bcd64f8259e03087fc70a
Joffrey	d2f272763efca04d0705fbb03ca84ab10329dc0419390a681ad07c6a1c3009f3	143e61e58870748ad1dedad5b19edebda07dd14bf5e350f5ab9fe73dc455cd90
Sansa	e8a5ecf39c3d5e2976d8achbf0e990fc9b8e1482128d1c2144c3f41693852c33f	65e62ab1cb47a2147d9e967c25a3baccf155effb3c2c130ec182483c2d85f350
Bran	051945a27551270c442208045a38bf38bf4c5b819fdb0f0511ceafa74a2af59	ae91d9bb0b1431816b493b019fd223bac23599b8e997b7db4e7ee81c4ee88526
Rickon	3b6de7f593f618cd6e02a51104419178036df9a20089e4c3cd579bc34025737d	3baef8a88edabd441a93fb34393ede71447166bab920f95974ca646ce9352786
Arya	b02e06485c54bb8d503d44ab75693665ccfb580a0d5cbd12c488d8c4aab51f37	6caa75389770a6e0c5898141d4098e13d122c0506625e8fdbeda8a1403e4865b

Question 3

Login	Hash - sha256(Password)	Password
tyrion	2a2fa6d7a8a83ca291b298a373fe602a2c2879c841a3bd8ef818d3cfaa9ecd40	beer11
littlefinger	f06f9c14c073e5b51503b6a4ecaccdee594420f60382b7c755d92ed4bdb6ee04	chaosladder

Question 4

Méthode suffixe	Suffixe de long. 2	Suffixe de long. 4
Dict. de taille 500	4 344	14 776 836
Dict. de taille 2 000	5 844	14 778 336
Dict. de taille 20 000	23 844	14 796 336

Méthode XKCD	Concat. De 2 mots	Concat de 3 mots	Concat de 4 mots
Dict. de taille 500	250 000	125 000 000	62 500 000 000
Dict. de taille 2 000	4 000 000	8 000 000 000	16 000 000 000 000
Dict. de taille 20 000	400 000 000	8 000 000 000 000	160 000 000 000 000 000