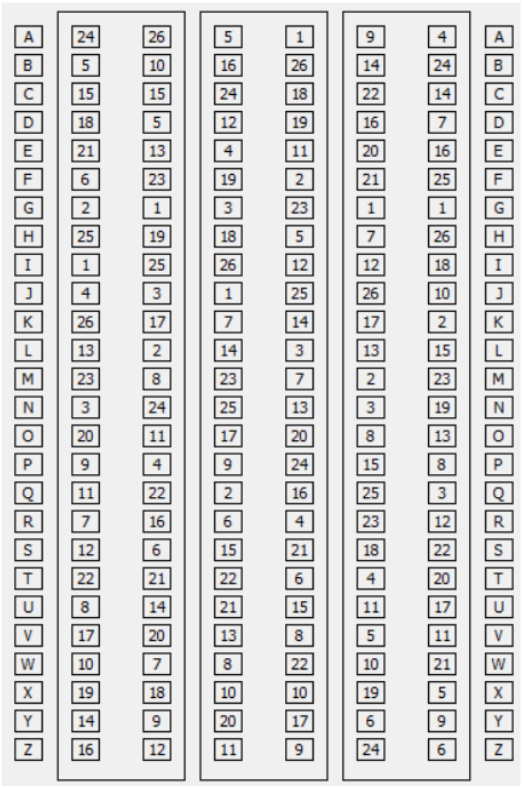
Испит из Заштите података (13E113ZP, 13S114ZP) – колоквијум 22.06.2020.

1. (**10п**) Нацртати и објаснити како се користећи криптографију са јавним кључем може истовремено постићи и тајност и аутентикација послате поруке. Да ли је могуће побољшати перформансе у делу који се односи на тајност, без нарушавања сигурности? Уколико је могуће, шта је потребно од додатних механизама и како би изменили почетну шему у том случају?

2. (**10п**) *Digital Authentication Algorithm* (DAA) је стари стандард за аутентикацију порука који је заснован на DES-CBC алгоритму. Данас се сматра да је несигуран и превазиђен је. Које су кључне мане овог алгоритма и на који начин су оне превазиђене код CMAC?

3. (**25п**) На слици је приказана тренутна конфигурација ротор машине приликом дешифровања неке веће поруке. До овог тренутка је дешифровано 308 карактера. Сматрати да ротори ротирају ка доле. Леви ротор ротира најбрже, док десни ротор ротира најспорије.

   а) (*4 поена*) Колико пута је ротирао сваки од ротора до овог тренутка? Објаснити.
   б) (*15 поена*) Приказати поступак дешифровања следећег дела веће поруке: *LVSFWMGJ*.
   ц) (*6 поена*) Нацртати почетну конфигурацију прва три реда ове ротор машине.

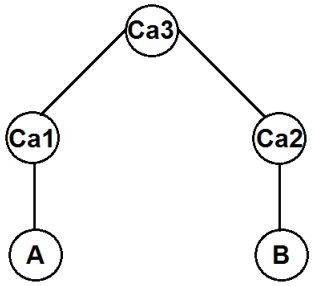


Напомена: *На колоквијуму нису дозвољена никаква помоћна средства, ни калкулатори ни литература. Колоквијум траје 70 минута.*

Испит из Заштите података (13E113ZP, 13S114ZP) – испит 22.06.2020.

1. **(15/10п)** Објаснити шта су и које су мане *Fixed* и *Anonymous Diffie Hellman* размена кључева које су се користиле у TLSv1.2.

2. **(15/10п)** Објасните како један учесник у комуникацији (A) који има сертификат издат од једног сертификационог ауторитета (Ca1) добија поуздан јавни кључ другог учесника у комуникацији (B), када је други учесник у комуникацији (B) добио сертификат од другог сертификационог ауторитета (Ca2), коришћењем хијерархије сертификационих ауторитета за пример са слике.



Слика 1. Пример хијерархије сертификационих ауторитета

3. **(25/15п)** *SMIME* протокол. Познато је да *SMIME* за обезбеђивање сваке функционалности може имплементирати више различитих алгоритама од којих су неки обавезни, а неки препоручљиви због веће сигурности. Укратко представити поступак избора алгоритма који се користи за имплементацију одређене функционалности када је то могуће.

Напомена: *На испиту нису дозвољена никаква помоћна средства, ни калкулатори ни литература. Испит траје 70 минута.*