Ehitame keeruliste salasõnade meeldejätmise asendamiseks luku, millega saab arvutisse sisse logida.

Arvutid nööpi

Nii, lugu valmis. Jääb veel skeemid ja koodid ajakirja FTP-saiti «üles» kupatada. Brausin sujuvalt FTP-lehele, aga… kes seda pagana salasõna enam mäletab? Oli teine igavene pikk ja keeruline. Paljud kasutavad paroolide salvestamiseks «välismälu» – paberlipikut, mis kleebitakse klaviatuuri alla või mõnda muusse «kindlasse» kohta. Mõni jälle kribab saladuse kuvari äärele. Nupukamad kasutavad mõne lause esitähti – lahendusi on palju, ent ükski pole nagu päris see õige. Aga kuidas oleks füüsilise võtmega?

Üks variant oleks kadunud firma Dallas (nüüdseks Maximi poolt alla neelatud) puutemälunööbi – *I-buttoni* – kasutamine. Kindlasti on paljudel lugejatel selline juba võtmekimbus kolisemas, sest päris paljude majade fonolukuga välisuksi saab avada sellise nööpmäluvõtmega. Laiendame selle imevõtme kasutusvõimalusi ja ehitame i-nööbi lugeja. Nööbilt loetav (unikaalne, 48-bitine) kood võib vabalt olla arvutisse ja miks ka mitte e-posti serverisse, ftp-saidile ja mujalegi sisselogimise salasõnaks. Sellest seekord juttu teemegi.

Bitid, baidid…

I-nööp on lihtsamal juhul tehases kirjutatud sisuga mälumikroskeem, mis sisaldab kaheksa baiti infot. Esimene infobait on nn perekonnakood ehk antud seadmete gruppi iseloomustav bait, i-nööpidel enamasti väärtusega 0x7F (kuueteistkümnendsüsteemis, rahvusvahelise lühendiga «hex»). Viimane number infojadas on loetu kontrollsumma. Selle järgi on hea loetu õigsust kontrollida (kuigi ma pole veel kordagi täheldanud, et järgnevas kirjeldatud kood oleks nööbilt infot välja pinnides eksinud). Usaldamatuses peitub jõud :)

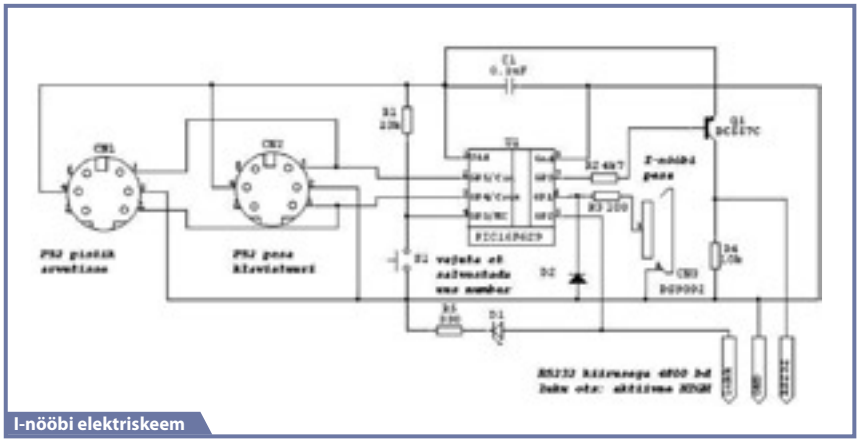
Kuus keskmist baiti ehk 48 bitti moodustavad iga tehaseväravast väljunud nööbi ainuomase salakoodi. Seda me kasutamegi.

Kavalamad ja kallimad nööbid toimivad muutmäluna, lubades endasse pikemaid tekste kirjutada. Sideprotokoll aga on kenasti sama ja seega toimiksid ka nemad meie sisselogimisviisardis ;) ilma probleemideta.

Lähemalt i-nööbist, sellega suhtlemisest ja vastavast etiketist võib lugeda veebilehelt www.ibutton.org. PICutajatest sõpru võiks rõõmustada teadmine, et Microchipi koduleht tutvustab nööbiga vestlemise koodinäiteid. Kindlasti leidub valmis koodijuppe ka AVR-idele ja teistele populaarsetele kontrolleritele. Ja kui ei leidugi, siis käesolevas koodis toodud algoritm sobib ikka, see tuleb vaid oma lemmiku progemiskeele süntaksis ümber kirjutada. See aga on juba suhteliselt lihtne töö.

! *PS. Moodsal ajal on moes igasugu juriidilist laadi märkused. Eks nad ole mõnikord vajalikudki, sest äkki mõni jänkistani algaja kõrvetab vidinat kokku jootes kolviga näppu ja kaebab sellepeale autori kohtusse ;) Seepärast disklaimer:*
Artiklis pakutud kood ja skeem on lugejatele vabaks kasutamiseks kas osade kaupa või tervikuna, nagu süda ihaldab ja milleks iganes. Assembleris mõistagi, see on asi, mille üle me ei vaidle. Kirjeldatu kasutamine kommertseesmärgil ilma autori kirjaliku loata on keelatud.

Ei autor ega toimetus kavatse vastutada seadme kasutamisest või kasutamata jätmisest tulenevate kahjude, looduskatastroofide, äkkrikastumise vms nähtuste eest.



I-nööbi elektriskeem

Lugejat on mugav ühendada arvuti klaviatuuri pessa ehk PS2-porti. Nii pole mingit muret seadme toitega, sest +5 V on sealses pesas täiesti olemas.

Töö algoritm

Lugeja toimimiseks pole vaja softi installida, registris sorida ega Linuxi make-failidest midagi teada. Lihtsalt pistik seina (antud juhul arvutisse) ja asi kombes.

Kuna skeem ühendatakse klaviatuuri vahele, läheb sealt loetud info samasse kohta, kuhu klaviatuuri omagi. Kui ekraanil on sisselogimisaken ja kursor asub parooliväljal, paneme nööbi lugejasse. LED-lugeja vilgatab korraks ja paroolivälja ilmub

kaheksa tärni. Need ongi i-nööbilt loetud unikaalne kood, perekonnakood ja kontrollsumma. Vajutame klahvi ENTER ja olemegi sisse logitud. Parooli esmakordsel sisestamisel tuleb toimida täpselt samamoodi.

Oot, aga kui avada tekstiredaktor ja siis võtit näidata? Salajane parool ilmub täies alastuses nähtavale? Jah, nii juhtub! Aga sama toimuks ka klaviatuurilt salasõna redaktorisse tippides. Seade polegi mõeldud üliturvaliseks ja kullakange sisaldava seifi ette teda panna võib-olla ei tasuks. Samas ei jäta ju keegi oma korterivõtmete kimpu niisama vedelema. Eriti veel sellisesse kohta, kus PICutajatest elektroonikahuvilisi ringi luusib.

Üks turvaauk on seadmel veel: nimelt on tehas salakoodi kenasti i-nööbikese peale pressinud. Fonolukkudes seda probleemiks ei peeta, aga seal pole ka klaviatuuri, kustkaudu midagi sisse toksida saaks. Salastatusastme suurendamiseks saab pärast pisikest käsitööd viiliga kirjest edukalt lahti. Ja jällegi – vastupidi laulusõnas soovitatule ütleksin: ärge jätke võtmeid väljapoole, siis pole ka tarvis nööbi pealt numbreid kraapida.

Mõni võte luku «muukimiskindluse» parandamiseks softis siiski on. Nimelt ei edasta lugeja porti kõikide nööpide koode, vaid ainult «oma». Uue võtme «lukuauku sobitamiseks» tuleb vajutada nuppu S1, seda all hoida ning siis näidata vana (juba lubatud) võtit. Tuluke süttib – masin on salvestusrežiimis. Nüüd tuleb «sisestada» uus i-nööp. Eduka lugemise korral tuli kustub ja kood on salvestatud. Kontrolliks avame oma lemmiktekstiredaktori ja paneme nööbi lugejale. Võrdleme ekraanile karanud märgijada nööbile trükituga – see peaks klappima.

Äsja valmis keevitatud lugeja protsessor ei tunne mõistagi ühtegi nööpi, neid pole ju veel tutvustatud. Õnneks on see nüüd rahumeeli nõus suvalist nööpi omaks võtma.

Kontrolleri programm jätab meelde kuni kahe võtme koodid. Kolmanda esitlemisel kustutatakse teine. Esimene võti jääb alati kehtivaks.

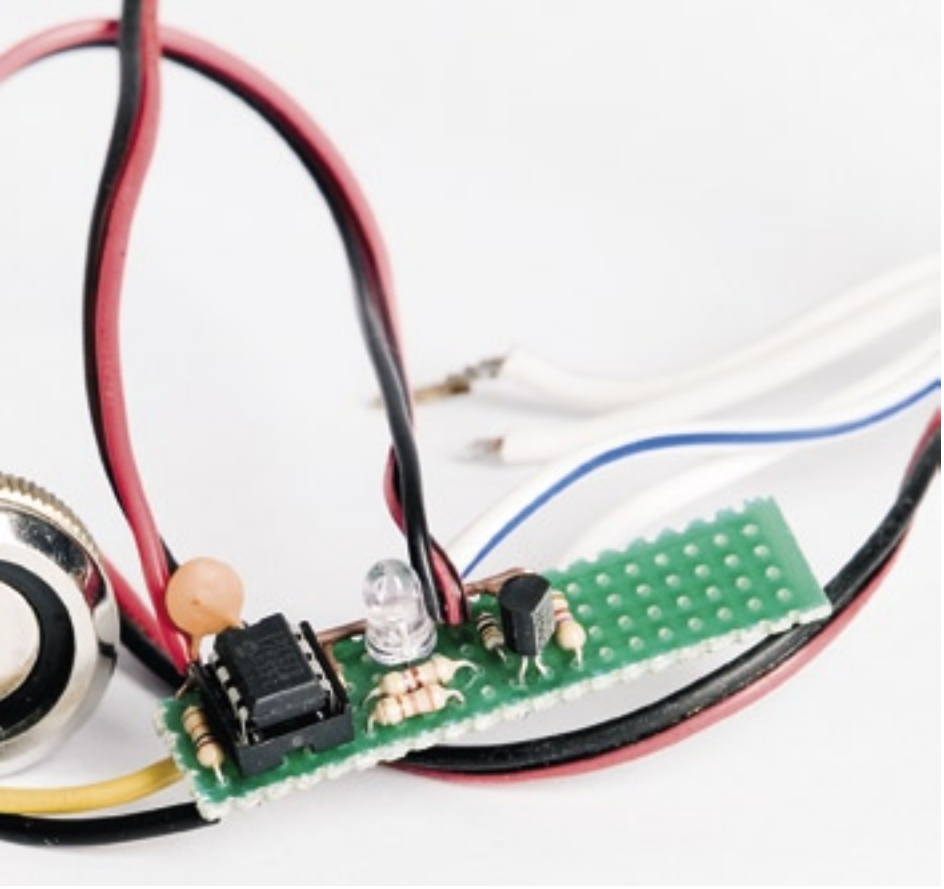
Aga kui tahame võtme keelata? Protseduur on sama, mis uue koodi salvestamisel, kuid selle erinevusega, et nüüd pannakse teisel korral lugeja pessa sama võti. LED kustub ja vaene PIC oleks nagu ajupesus olnud – kõik paroolid kustutatud. Kuni uue i-nööbi koodi salvestamiseni edastatakse porti suvaliselt pessa CN3 surgatud nööbilt loetav.

Skeem

Salaluku skeem on lihtne, see sisaldab vaid PIC-protsessorit ning paari takistit. Pistikupesa CN3 on i-nööbi pesa. Seda detaili saab osta elektroonikapoest, kuid sama hea asja saab väänata paarist plekitükist. Paarsada krooni nagu maast leitud! Nööp ise maksab näiteks ELFA kataloogist tellides umbes 65 raha.

Kondensaator C1 surub maha võimalikke impulsshäireid mikroskeemi toiteahelas ja R1 hoiab PIC sisendi 4 kõrgel nivool (see on

Detail	Tähis skeemil	Nominaal	Kogus	Märkus/tootekood
Pistik/pesa	CN1	-	1	DIN-6-pistik kaablile (vajadusel)
	CN2	-	1	DIN-6-pesa kaablile (vajadusel)
	CN3	DS9092	1	I-nööbi pesa, ELFA kood: 73-766-84, vajadusel
Pooljuhid	U1	PIC12F629	1	
	Q1	BC557C	1	
	D1	Meelepärane LED	1	
	D2	1,5KE400CA	1	Ülepinge kaitsediood
	-	DS1990A	Vastavalt kasutajate arvule	I-nööp (vajadusel) Tevalo kood: 302-967
Kondensaatorid	C1	100nF	1	
Takistid	R1	10k	1	Suvalise võimsusega
	R2	4,7k	1	
	R3	100	1	1 W või võimsam
	R4	10k	1	Suvalise võimsusega
	R5	330	1	
Muud	S1	-	1	Vajutamisel sulguvate kontaktidega nupp



ainus koib, millel pole kivi ehk nn *pull-up*-takistit sees).

Takisti R3 kaitseb protsessorit piirates võimaliku staatilise elektri impulsi tekitatud voolu. D2 täidab sarnast funktsiooni. Põhimõtteliselt võib nimetatud detailid ka skeemist ära jätta, kuid siis on oht, et ühel kenal päeval pärast kammi klaverile lennutamist jääb arvutisse sisselogimine ära ning tuleb poodi uue kivi järele minna.

Muide, seadet saab edukalt kasutada toaukse lukuna. Viimase elektrilisele vasturauale saab signaali otse LED-i tüürivast ahelast. Vahele tuleks ehitada paari transistori või mikroskeemiga ULN2003 puhvervõimendi, sest pisike PIC ei suuda suurt võimsust nõudvat taba omal käel tüürida.

Vana hea järjestikpordi austajate jaoks väljastatakse I-buttonilt loetud kood ka RS-232 nivooga. Saatmiskiirus 4800bd. Nivoomuundur on realiseeritud transistoril Q1 ja takistitel R2, R4. Väga korrektne selline lülitus just pole, kuid siiski kasutatav. Vajadusel võib sisse viia «päris» puhvrikivi MAX232. Kui järjestikinfot ei vajata, saab Q1 ja takistid R2 ning R4 skeemist välja visata.

Montaaž

Monteerime lugeja vähesed detailid makettplaadijupikesele ja programmeerime PIC (või tellime juba programmeeritu ajakirja toimetusest). Iseprogrammeerijad leiavad koodi ja programmi lähteteksti, nagu alati, ajakirja FTP-serverist (ftp.arvutikasutaja.ee/rauakool).

Kui omatehtud nööbipesa kukkus kenakene välja, võiks selle kruvida otse klaviatuuri külge. Jälle üks tüütu juhe vähem, neid tolkneb masina küljes niigi ülemäära palju. DIN-6 pistiku/pesa paari pole siis ka tarvis. Nupp S1 mahub näiteks klaveri tagaküljele.

Enne skeemi arvuti porti surkamist kontrollime, et toiteahelas ei oleks lühist, sest muidu põleb maha PC emaplaadil olev kaitse. Samuti tasub veenduda, et toiteotsad said õigetpidi joodetud, sest PIC lehvitab vale polaarsusega pinge korral hüvastijätuks nukralt koiba ja lahkub... igaveseks.

Muud nagu ei olegi, pinge peale ja *login*!

Veljo Sinivee
felch@staff.ttu.ee

Märkused

- Nagu eespool kirjas, pole i-nööbiga sisselogimine just üliturvaline. Nööbilt loetavat parooli saab vaadata suvalise tekstiredaktoriga. Tõsi, siis peaks nuhkijal nööp ja lugeja käepärast olema.
- Nööbi number on tehases vidina peale pressitud. Võiks muidugi öelda, et ka mehaanilise luku võtme hammaste kuju on kõigile näha, kuid turvarisk on see ikkagi. Ärge jätke võtmeid väljapoole.
- Ei ole hea kasutada igal pool ühte ja sama parooli. Kui see peaks halva inimese kätte juhtuma, on tal juurdepääs kõigele. Üks võimalus oleks tippida nööbilt loetava jada lõppu veel mingi number, mis oleks igas parooli küsivas kohas erinev. Erinevate nööpide kasutamine oleks samuti mõeldav, kuid natuke tülikas.