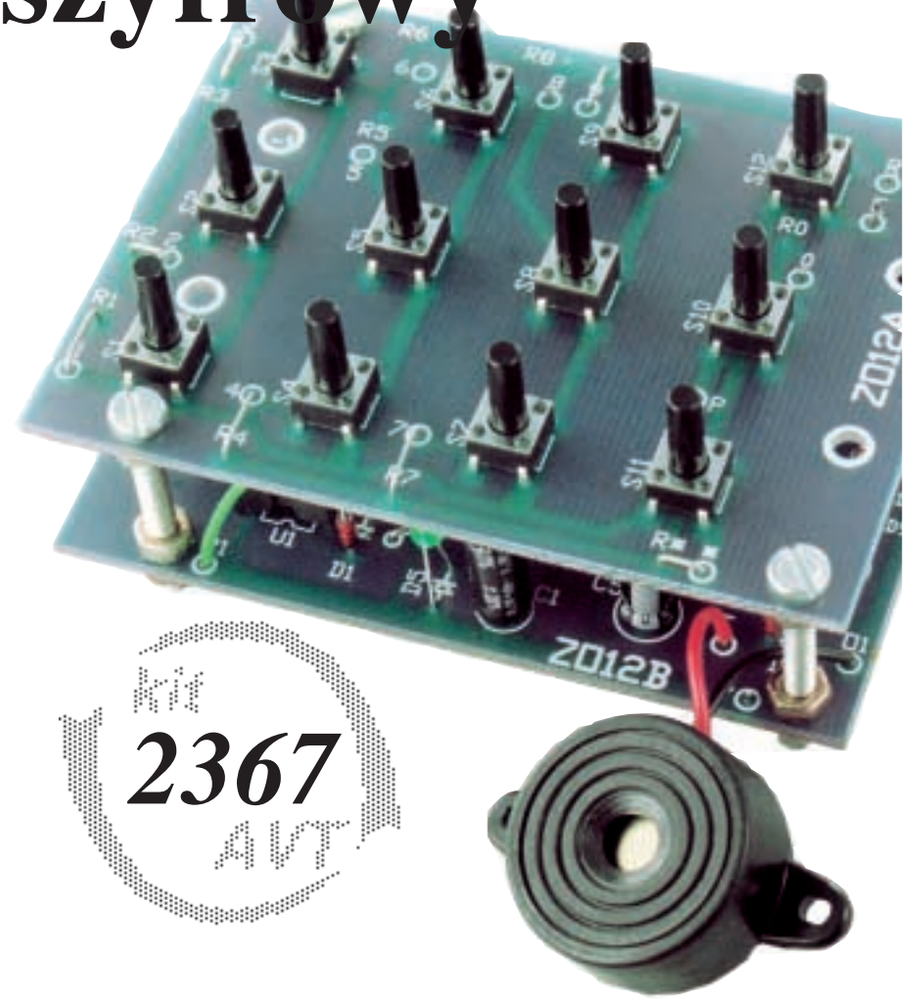
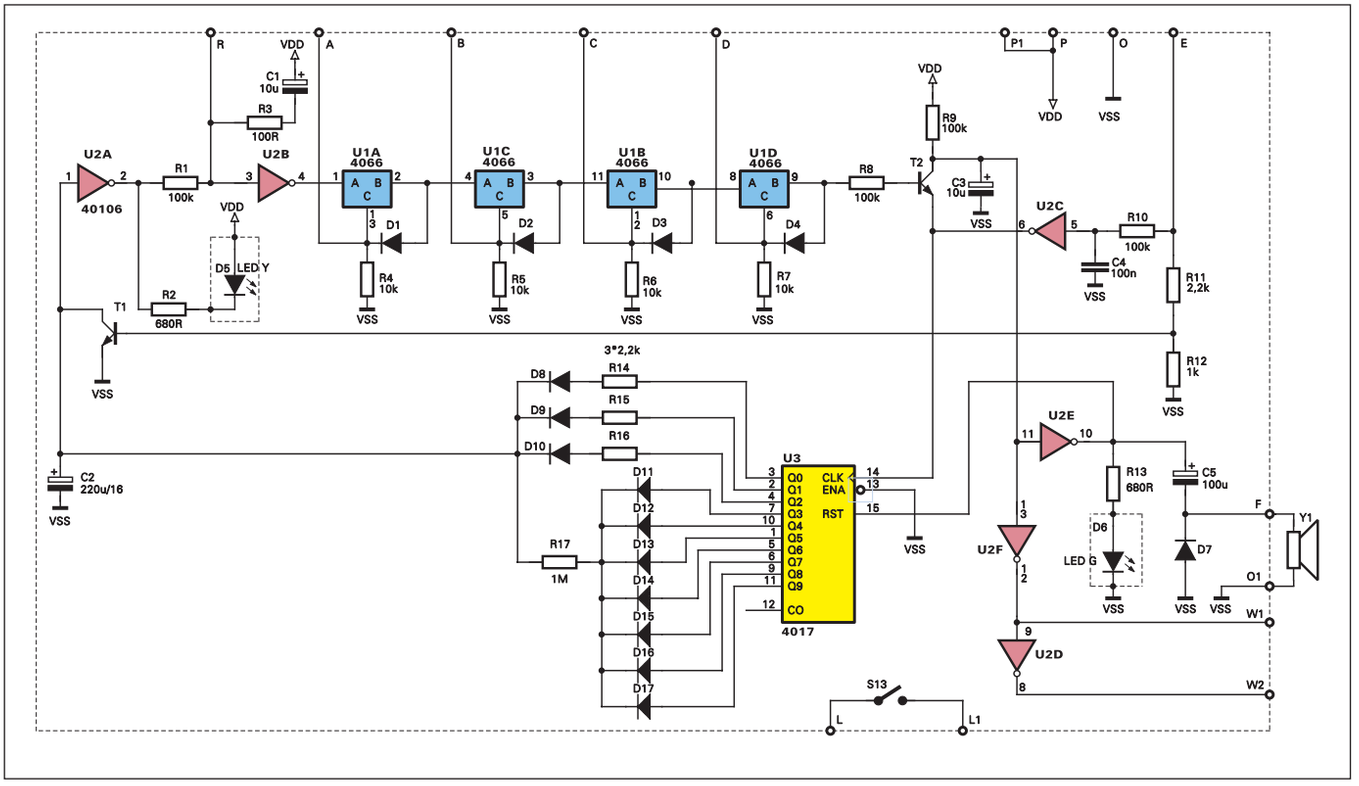
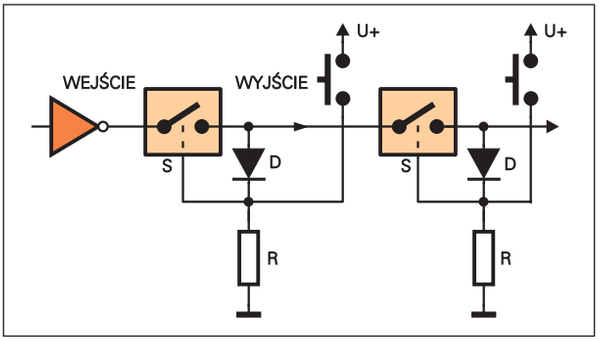
Zamek szyfrowy



Nadesłane do Redakcji ankiety pokazały, że istnieje duże zapotrzebowanie na prosty zamek szyfrowy. W artykule opisano układ zrealizowany z użyciem kilku popularnych kostek CMOS i dwunastoklawiszowej klawiatury. Pomimo prostoty układowej urządzenie ma cenne właściwości, charakterystyczne dla sprzętu profesjonalnego. Zamek wymaga podania czterocyfrowego kodu. W przypadku pomyłki (naciśnięcia niewłaściwego klawisza) układ jest zerowany i wymaga powtórnego wprowadzenia kodu. Jeśli trzykrotnie zostanie wprowadzony niewłaściwy kod, układ zostaje zablokowany na dłuższy czas (kilka minut). Ponowne wprowadzenie kodu jest możliwe dopiero po upływie tego czasu. Taka blokada praktycznie uniemożliwia odnalezienie właściwego kodu metodą chybił-trafił. A długi czas blokowania skutecznie znie-



Rys. 1 Schemat ideowy układu głównego



Rys. 2 Zasada działania

chęci do prób szukania prawidłowego kodu metodą prób i błędów.

Pomimo pełnienia takich zaawansowanych funkcji, sam układ elektroniczny jest bardzo prosty, dlatego jego wykonanie i uruchomienie nie powinno nikomu sprawić trudności.

Opis układu

Rysunek 1 pokazuje schemat ideowy części elektronicznej zamka. Główną rolę pełni tu zespół czterech kluczy analogowych popularnej kostki U1 CMOS 4066. Klucze pracują tu w roli zatrzasków, zapamiętujących naciśnięcia kolejnych klawiszy. Klawisze te powodują podanie stanu wysokiego (plusa zasilania) na punkty oznaczone A, B, C, D. Rysunek 2 tłumaczy zasadę działania. Jak wiadomo, klucz analogowy zostanie zwarty wtedy, gdy na elektrodę sterującą oznaczoną S zostanie podany stan wysoki. Jeśli na wejściu układu z rysunku 2 napięcie jest bliskie masy, klucz będzie otwierany tylko na czas naciskania przycisku, ale się nie "zatrzaśnie". Klucz analogowy zostanie otwarty na stałe tylko wtedy, gdy na wejściu danego klucza panuje stan logiczny wysoki (napięcie bliskie plusa zasilania) i jednocześnie zostanie przyciśnięty współpracujący przycisk. Tym razem nawet krótkie naciśnięcie przycisku spowoduje trwałe pojawienie się na wyjściu stanu wysokiego. Stan ten zostanie podany na wejście następnego klucza, który teraz może zostać otwarty na stałe po naciśnięciu współpracującego z nim przycisku. Dołączenie kilku kolejnych takich samych stopni pozwoli zbudować układ zamka szyfrowego, uruchamianego naciskaniem kolejno odpowiednich przycisków. Są to przyciski dołączone do punktów A, B, C, D układu z rysunku 1. Rysunek 3 pokazuje schemat ideowy uniwersalnej klawiatury współpracującej z układem z rysunku 1. Układ znaków jest tu taki sam, jak w klawiaturze telefonicznej, występują także dwa dodatkowe przyciski oznaczone * i # (S11 i S12).

Należy zauważyć, że warunkiem prawidłowego działania jest stała obecność stanu wysokiego na wejściu pierwszego klucza (nóżka 1 układu U1A). Tym samym taki zestaw może być w prosty sposób wyzerowany przez chwilowe zabranie z tego wejścia stanu wysokiego. Wtedy wszystkie klucze zostaną otwarte (o ile nie są naciśnięte współpracujące z nimi przyciski). Ta właściwość jest wykorzystywana do zerowania łańcucha kluczy w przypadku naciśnięcia niewłaściwego przycisku.

Jak widać na rysunkach 1 i 3, użytkownik może sam zaprogramować hasło-kod, łącząc cztery przyciski klawiatury numerycznej z czterema wejściami oznaczonymi A, B, C, D. W praktyce hasłem-kodem będzie czterocyfrowa liczba.

Aby system nie był łatwy do "złamania", wszystkie klawisze nieużywane w haśle-kodzie należy podłączyć do punktu oznaczonego R. Wtedy naciśnięcie jakiegokolwiek nieprawidłowego klawisza spowoduje szybkie rozładowanie dotychczas naładowanego kondensatora C1 przez małą rezystancję R3. Na wyjściu bramki U2B pojawi się stan niski i nastąpi wyzerowanie zestawu czterech kluczy.

Kolejnym utrudnieniem w "złamaniu" kodu jest obecność obwodu współpracującego z klawiszem oznaczonym #. Przycisk # zawsze musi być dołączony do wejścia E na płytce głównej. Otwarcie zamka nie następuje bezpośrednio po wprowadzeniu odpowiedniego hasła-kodu - trzeba dodatkowo nacisnąć przycisk #. Dopiero to spowoduje pojawienie się na wyjściu (wyjściach) stanu aktywnego czyli mówiąc krótko - otwarcie zamka.

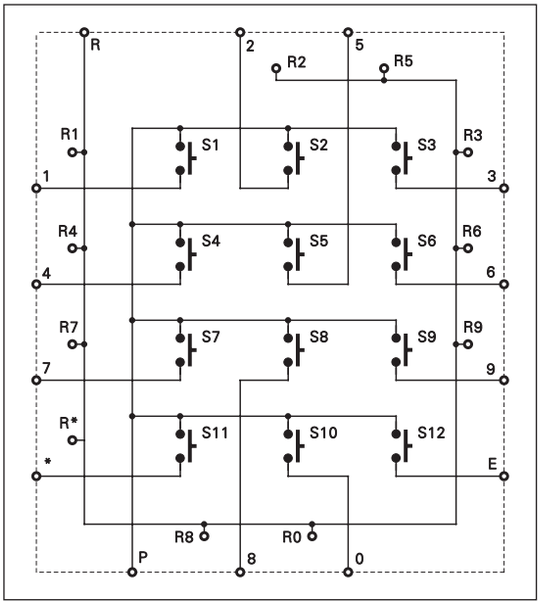
Działanie tego obwodu jest następujące. Naciśniecie przycisku # spowoduje pojawienie się stanu niskiego na wyjściu bramki U2C (nóżka 6). Umożliwia to pracę tranzystora T2. Jeśli wcześniej został wprowadzony właściwy kod, tu wszystkie klucze analogowe są otwarte, przewodzą i w konsekwencji tranzystor T2 zostaje otwarty. Otwarcie tranzystora T2 powoduje rozładowanie kondensatora C3 i podanie stanu niskiego na bramki U2E i U2F.

Powoduje to pojawienie się stanu wysokiego na wyjściu bramki U2E , włączenie zielonej diody LED D6 i włączenie brzęczyka piezo na krótki czas ładowania kondensatora C5. Krótki pisk brzęczyka i świecenie zielonej diody D6 informują, że zamek został otwarty. Jednocześnie stan wysoki pojawia się na wyjściu W1. Dodatkowy inwerter U2D daje w tym czasie na wyjściu W2 stan niski. W zależności od potrzeb, może być wykorzystane dowolne z wyjść W1, W2. W dalszej części artykułu będzie wykazane, że stan aktywny na tych wyjściach i czas świecenia diody D6 wyznaczony jest głównie przez stałą czasową obwodu R9C3, a wbrew pozorom nie zależy od czasu naciskania przycisku #. Obwód opóźniający R9C3 wprowadzono głównie po to, by sygnał aktywny nie był zbyt krótki nawet przy krótkim naciśnięciu tego przycisku.

Ważną rolę pełni także obwód R11, R12, T1. W stanie spoczynku kondensator elektrolityczny C2 jest naładowany. Na wyjściu bramki U2A panuje stan niski. Żółta dioda LED D5 świeci, wskazując, że układ jest w stanie oczekiwania i można wprowadzać kod. Na wyjściu bramki U2B panuje stan wysoki, umożliwiający prace zespołu kluczy analogowych kostki U1.

Po naciśnięciu klawisza # tranzystor T1 przewodzi i szybko rozładowuje kondensator C2. Na wyjściu bramki U2A pojawia się stan wysoki, gaśnie żółta dioda sygnalizująca gotowość. Dotychczas naładowany kondensator C1 zaczyna się rozładowywać przez R1. Po czasie wyznaczonym przez R1C1 (ok. 1 sekundy) na wyjściu bramki U2B (nóżka 4) pojawia się stan niski, który zeruje zestaw kluczy.

Co istotne, takie opóźnione zerowanie następuje po każdym naciśnięciu przycisku #. Uniemożliwia to złamanie kodu przez trwałe naciśnięcie klawisza # i próby znalezienia w tym czasie właści-



Rys.3 Schemat klawiatury

wego kodu metodą prób i błędów. Jest to niemożliwe, bo trwałe naciśnięcie klawisza # rozładowuje kondensatory C2, C1 i uniemożliwia pracę zespołu kluczy kostki U1. Sygnalizuje to dioda gotowości D5, która jest na ten czas wygaszana.

Układ powróci do stanu gotowości dopiero po naładowaniu się kondensatorów C1 i C2. Aby to nastąpiło, przycisk # musi zostać zwolniony. Tranzystor T1 zostanie zatkany i kondensator C2 zacznie się ładować prądem płynącym z wyjścia Q0 licznika U3 przez rezystor R14 i diodę D8. Najpierw zmieni stan bramka U2A i zaświeci żółta dioda gotowości, a mniej więcej sekundę później naładuje się C1, zezwalając na pracę zespołu kluczy.

Jak wynika z opisu, rzeczywista gotowość zespołu kluczy analogowych wystąpi mniej więcej w sekundę po zapaleniu diody gotowości D5. Jak z tego widać, w czasie tej dodatkowej sekundy nie należy podawać kodu. Wbrew pozorom nie jest to znacząca wada, bowiem właściwość ta daje o sobie znać tylko wtedy, gdy pierwszy podany kod był błędny. Uprawniony użytkownik w razie pomyłkowego podania błędnego kodu raczej nie będzie się spieszył i starannie, pomału wybierze prawidłowy numer, a wspomniane sekundowe opóźnienie nic mu nie przeszkodzi.

W tym miejscu należy przestrzec wszystkich racjonalizatorów, którzy dla zlikwidowania tej właściwości chcieliby włączyć diodę D5 na wyjściu bramki U2B. Byłby to bardzo nierozsądny krok, ponieważ wtedy dioda D5 pozwoliłaby łatwo określić, które klawisze są niewykorzystane w haśle-kodzie.

Aby jeszcze bardziej zwiększyć odporność systemu na "złamanie" wprowadzono dodatkowy obwód z licznikiem U3. Każde uruchomienie przycisku # powoduje podanie impulsu na wejście zegarowe (nóżka 14). Jeśli wprowadzono prawidłowy kod, licznik nie zwiększa jednak swego stanu, ponieważ od razu jest zerowany podaniem stanu wysokiego na wejście zerujące RST (nóżka 15). Jeśli jednak przycisk # został naciśnięty po wprowadzeniu nieprawidłowego kodu, zerowanie nie nastąpi i licznik zwiększy swój stan o jeden. Tym samym stan wysoki "przeskoczy" z wyjścia Q0 na wyjście Q1 (nóżka 2). Nie spowoduje to istotnej zmiany właściwości układu. Podobnie podanie niewłaściwego kodu po raz drugi, zwiększy stan licznika, powodując przeskoczenie "jedynki" na wyjście Q2.

Sytuacja zmieni się radykalnie dopiero po trzecim podaniu błędnego kodu (i trzecim naciśnięciu przycisku #). Pojawienie się stanu wysokiego na wyjściu Q3 spowoduje, że po zwolnieniu przycisku #, kondensator C2 będzie się ładował nie przez małe rezystancje R14-R16, tylko przez dużą rezystancję R17. Będzie to trwać kilka minut (3...5) i w tym czasie system będzie zablokowany, o czym świadczyć będzie wygaszona dioda D5. Tym samym czwarta próba wprowadzenia kodu będzie możliwa dopiero po kilku minutach. Tak samo piąta i następne próby będą możliwe po kolejnych kilku minutach. Obecność licznika U3 na pewno zniechęci każdego, kto chciałby znaleźć kod metodą prób i błędów.

W układzie modelowym wszystkie rezystory R14-R16 mają jednakową wartość. Niektórzy użytkownicy prawdopodobnie uznają., że już drugie i trzecie opóźnienie należy zwiększać i rezystor R15 powinien mieć zauważalnie większą wartość, na przykład 10 czy 22kΩ, a R16 jeszcze więcej, w granicach 47...220kΩ. Ta sprawa leży w gestii wykonawcy tego układu.

Jak wynika z dokładnej analizy układu, impulsy na wyjściach W1 i W2 mają czas trwania wyznaczony jest przede wszystkim przez elementy R1C1 i czas ładowania przez C3. W przypadku ładowania kondensatora C3 po zwolnieniu przycisku # (gdy na wyjściu U2C panuje stan wysoki) trzeba wziąć pod uwagę nie tylko rezystor R9, ale również ładowanie w obwodach R8-złacze B-C tranzystora oraz E-B-C tranzystora T2. Czas trwania impulsów wyjściowych nie zwiększy się przy dłuższym naciskaniu przycisku #, ze względu na rozładowanie kondensatorów C2 i co istotniejsze C1.

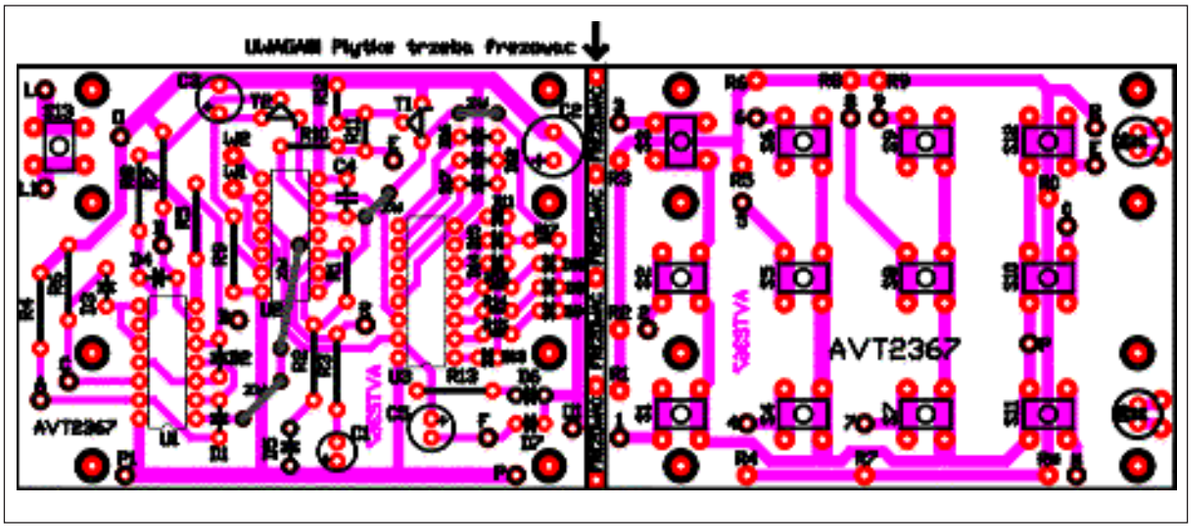
Na schemacie ideowym zaznaczono dodatkowy przycisk S13. W urządzeniach alarmowych powszechnie stosuje się taki przycisk antysabotażowy, który uruchamiany w przypadku zdjęcia obudowy sygnalizuje włamanie do wnętrza danego urządzenia, w tym przypadku zamka szyfrowego.

Montaż i uruchomienie

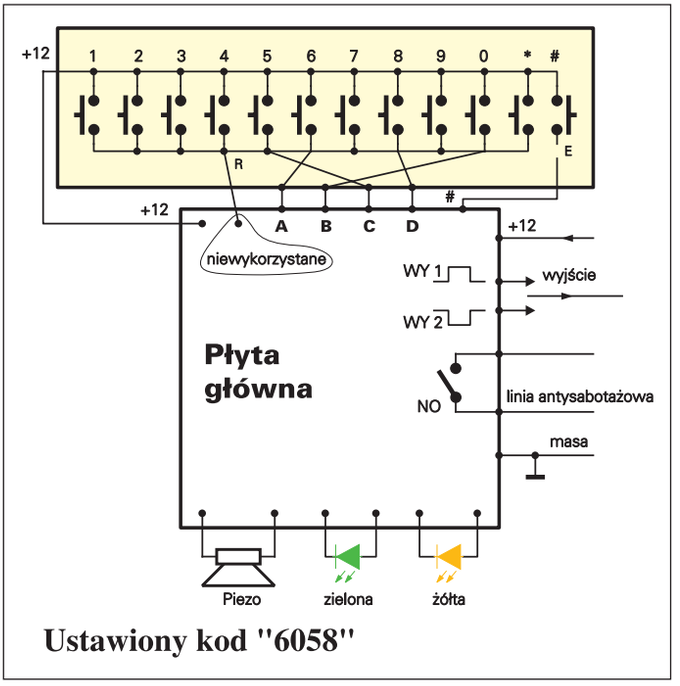
Pokazany układ można bez większego trudu zmontować na dwóch płytkach drukowanych. Główna płytka z cała elektroniką pokazana jest na **rysunku 4**.

Montaż dolnej płytki z całą elektroniką nie powinien sprawić trudności. Zgodnie z ogólnymi zasadami należy najpierw zmontować zwory, leżące rezystory, a potem kolejne elementy coraz większe, bierne i czynne. Ze względu na wymaganą niezawodność zaleca się wlutowanie układów scalonych bezpośrednio w płytkę, bez stosowania podstawek. Miejsce na przycisk antysabotażowy S13 przewidziano na płytce. Może to być zwykły microswitch, rozwierany przy rozłączeniu płytek, ale lepiej będzie zastosować inny przełącznik, chroniący raczej obudowę, rozwierany w przypadku jej otwarcia czy uszkodzenia.

Druga płytka, przedstawiona na **rysunku 5** zawiera przykładową klawiaturę podobną do telefonicznej. W roli klawiszy zastosowano tu dwanaście popularnych microswitch'ów. Przycisk S12 (wcześniej wspominany #) zawsze będzie przyciskiem zatwierdzającym. Pozo-



Rys. 4 i 5 Schemat montażowy



Rys. 6 Układ połączeń

stałe znaki: cyfry 0-9 i gwiazdkę (*) można dowolnie wykorzystać do zaprogramowania hasła-kodu. W tym celu odpowiednie końcówki wybranych przycisków należy dołączyć do punktów A...D płyty głównej. Pozostałe niewykorzystane klawisze należy połączyć z punktem R płyty głównej. Na płytce z rysunku 5 przewidziano zwory, które znakomicie ułatwią to zadanie. Należy wlutować zwory przy wszystkich niewykorzystanych przyciskach, pamiętając, że oznaczenie R0...R9 i R* na rysunkach 3 i 5 nie oznaczają rezystorów, tylko punkty obwodu zerowania R. Pomocą może też być fotografia modelu, gdzie brakuje zwór przy znakach 0, 5, 6, 8, ponieważ wybrane hasło-kod to liczba 6058. Z kolei rysunek 6 pokazuje niezbędne połączenia w przypadku ustawienia kodu "6058". Jak wynika z **rysunku 6**, obie płytki można połączyć elektrycznie za pomocą siedmiu przewodów (plus zasilania oraz punkty A, B, C, D, E, R), a mechanicznie za pomocą trzech czy czterech śrub z nakrętkami lub tulejami dystansowymi. Taki "kanapkowy" zestaw należy umieścić w odpowiedniej obudowie. Nie powinno to być problemem, bowiem w obu płytkach przewidziano osiem dużych otworów do łączenia płytek ze sobą i z obudową. W ostateczności można zastosować obudowę z tworzywa sztucznego, ale zdecydowanie bardziej należy zalecić obudowę metalową, by ewentualny włamywacz nie zdecydował się na jej mechaniczne uszkodzenie.

W przedniej płycie obudowy należy wywiercić otwory na przyciski. Na przedniej płycie należałoby także umieścić naklejkę z cyframi 1...9, 0 i znakami * i #. Przykładowa naklejka czołowa pokazana jest na **rysunku 7**.

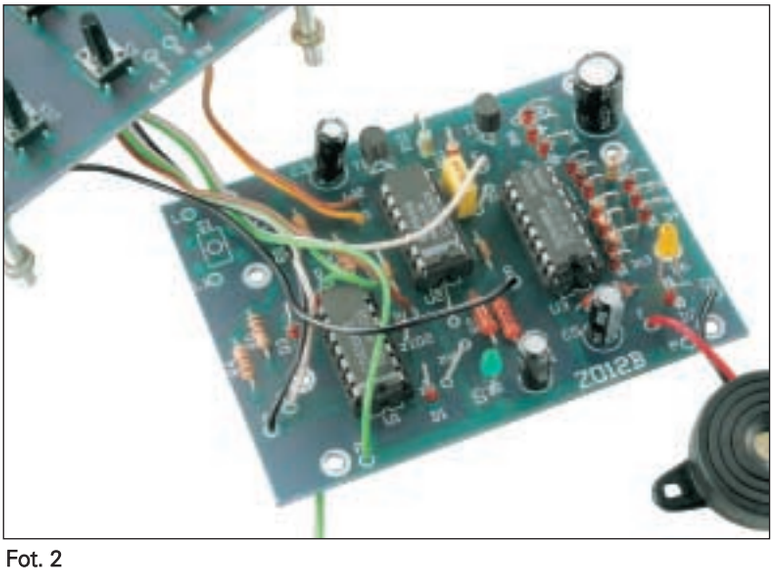
W przypadku umieszczenia układu na zewnątrz domu, trzeba zadbać o odpowiednie zabezpieczenie przez czynnikami atmosferycznymi, zwłaszcza deszczem i wilgocią. Należy jednak pamiętać, że układ nie był testowany w temperaturach do -20°C, choć biorąc pod uwagę zastosowane elementy, przy odpowiednim zabezpieczeniu silikonem czy lakierem powinien pracować także w tak niskich temperaturach, a zmianie mogą ulec tylko czasy opóźnienia wyznaczone przez kondensatory elektrolityczne. Przy pracy w trudnych warunkach należałoby też zastosować inną klawiaturę - zamiast prostych microswitch'ów użyć przycisków wyższej klasy, najlepiej hermetycznych i zdecydowanie bardziej trwałych. Godne rozważenia jest użycie klawiatury telefonicznej, przy czym najprawdopodobniej trzeba będzie zmienić układ połączeń, by był zgodny z rysunkiem 3.

Kodowanie hasła

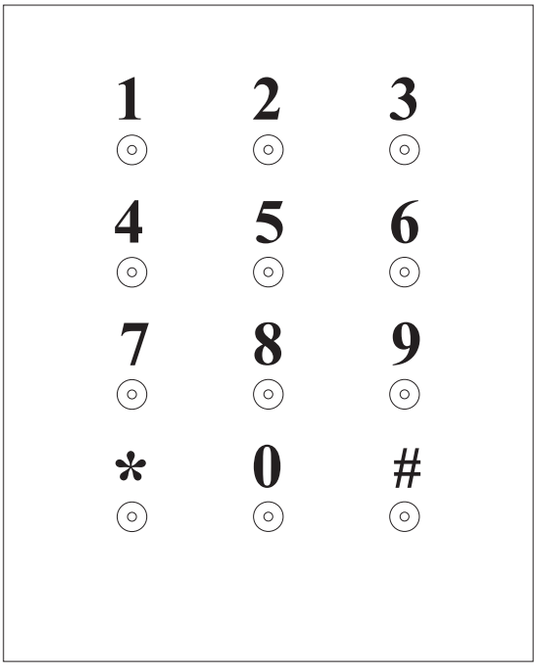
Przy kodowaniu numeru zaleca się, by wszystkie cyfry były różne, czyli żadna z nich nie powinna się powtarzać.

W żadnym wypadku kod nie powinien składać się z jednakowych cyfr, np. 4444, bo układ zostanie otwarty po jednorazowym naciśnięciu klawisza 4. Podobnie nie należy stosować powtórzenia tej samej cyfry, na przykład 3662, bo zmniejsza to liczbę aktywnych cyfr kodu z czterech do trzech.

W praktyce koniecznie trzeba też wziąć pod uwagę wycieranie przycisków wskutek częstego używania. Jest to poważny problem dotyczący także najbardziej wymyślnych, profesjonalnych szyfratorów. Z czasem okazuje się, ze używane klawisze są wytarte, natomiast kla-



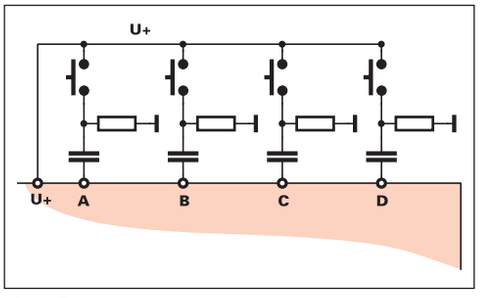
Fot. 2



Rys. 7 Naklejka

wisze nieużywane są zużyte w zauważalnie mniejszym stopniu. Dla potencjalnego włamywacza stanowi to istotną wskazówkę, jakie cyfry wchodzą w skład kodu. Złamanie takiego "wytartego" szyfratora jest zdecydowanie łatwiejsze, bo polega zna znalezieniu właściwej kombinacji tylko kilku klawiszy. Z tego też względu nie zaleca się używania dwukrotnie tej samej cyfry, na przykład 2727, ponieważ biorąc pod uwagę wytarcie klawiszy włamywacz z łatwością złamie szyfr wiedząc, że kod składa się tylko z cyfr 2 i 7. W opisywanym układzie wspomniany problem występuje z całą ostrością, ponieważ wielokrotne naciskanie takich wytartych, czyli używanych klawiszy w przypadkowej kolejności doprowadzi w końcu do włączenia wszystkich czterech kluczy analogowych, a późniejsze naciśnięcie klawisza # otworzy zamek.

Aby nie ułatwiać złamania kodu, należy albo zastosować klawiaturę odporną na wycieranie (co w praktyce wcale nie jest łatwe), albo prościej - co kilka miesięcy zmieniać kod wejściowy. Wtedy opisany zamek będzie naprawdę bardzo "trudny do złamania".



Rys. 8 Obwody dodatkowe

Omawiając kwestię złamania kodu należy koniecznie wspomnieć o sposobie polegającym na wciśnięciu na raz wszystkich klawiszy. W przypadku wykorzystania wejścia R (do którego podłączone winny być wszystkie nieużywane klawisze), jednoczesne naciśnięcie całej klawiatury nie spowoduje otwarcia zamka. Jednak w przypadku jednoczesnego naciśnięcia tylko klawiszy wytartych, używanych, zamek zostanie otwarty. Daje tu o sobie znać wspomniana wcześniej zauważalna wada opisanego prostego układu. Prostą metodą poprawiającą skuteczność zabezpieczenia jest zastosowanie czterech dodatkowych obwodów różniczkujących RC na wejściach kodowych A...D według rysunku 8. Stała czasowa RC tych obwodów, ustalająca długość "szpilki" powinna być krótka, poniżej 1ms. Wtedy nawet naciśnięcie w tym samym czasie wszystkich używanych, wytartych klawiszy nie otworzy zamka. Ze względu na krótki czas trwania "szpilek", nie ma szans, by nacisnąć cztery klawisze dokładnie w tej samej chwili, by wszystkie te szpilki pojawiły się idealnie w tym samym czasie z dokładnością do ułamka milisekundy.

Opisywany sposób z dodatkowymi obwodami RC uniemożliwia co prawda otwarcie w przypadku jednoczesnego naciskania wszystkich wytartych klawiszy, jednak nie stanowi zabezpieczenia przed złamaniem kodu przez wielokrotne naciskanie używanych, wytartych klawiszy w przypadkowej kolejności. Z tego względu w opisanym układzie zrezygnowano z opcji pokazanej na rysunku 8.

Na koniec należy przypomnieć, że problem "wytartych klawiszy" w mniejszym lub większym stopniu dotyczy wszelkich zamków cyfrowych posiadających klawiaturę, i jedynym prostym i skutecznym sposobem uniknięcia tego zjawiska są okresowe zmiany kodu.

Wykaz elementów

Rezystory
- R1,R8-R10: 100kΩ
- R2,R13: 680Ω
- R3: 100Ω
- R4-R7: 10kΩ
- R11,R14-R16: 2,2kΩ
- R12: 1kΩ
- R17: 1MΩ

Kondensatory
- C1,C3: 10µF/16V
- C2: 220µF/16V
- C4: 100nF
- C5: 100µF/16V

Półprzewodniki
- D1-D4,D7-D17: 1N4148
- D5: LED żółta
- D6: LED zielona
- T1,T2: dowolny NPN (np.BC548B)
- U1: 4066
- U2: 40106
- U3: 4017

Pozostałe
- Y1: piezo z gen.
- S1-S13: mikroswitch

Komplet podzespołów z płytką jest dostępny w sieci handlowej AVT jako kit AVT-2367

Reklama • Reklama • Reklama • Reklama • Reklama • Reklama • Reklama • Reklama • Rek