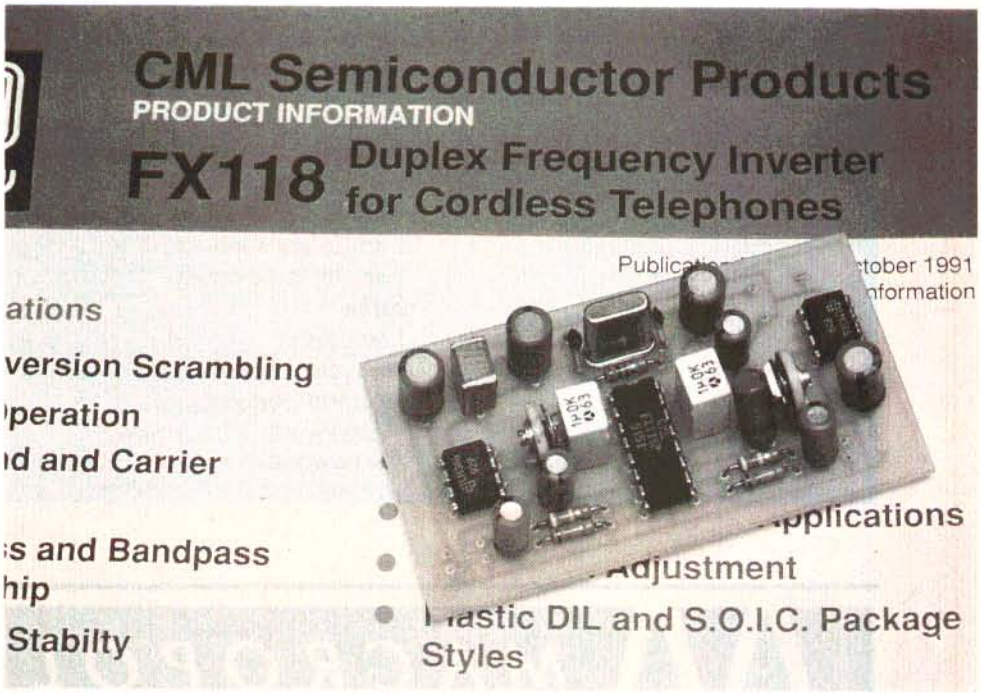
Szyfrator rozmów telefonicznych

Fakt stosowania podsłuchu rozmów telefonicznych - czy to legalnie, w ramach procedury prawnej, czy nielegalnie, pod jakimkolwiek pretekstem - jest powszechnie znany. Zagrożenie podsłuchem istnieje w przypadku łączności telefonicznej, ale szczególnych rozmiarów nabiera w przypadku przesyłania rozmów drogą radiową - dotyczy to zarówno telefonów samochodowych, radiowej łączności morskiej jak telefonii bezprzewodowej. Szyfrowanie rozmów jest proste z punktu widzenia techniki. Przepisy prawne zabraniają jego stosowania, gdy utrudnia działalność funkcjonariuszom służb państwowych, a zezwalają na nie, gdy oddaje tym samym funkcjonariuszom usługi. Tymczasem powszechna dostępność specjalizowanych układów scalonych stwarza nader silną pokusę wykorzystania ich w konstrukcji urządzeń szyfrujących...



Dlaczego szyfrowanie

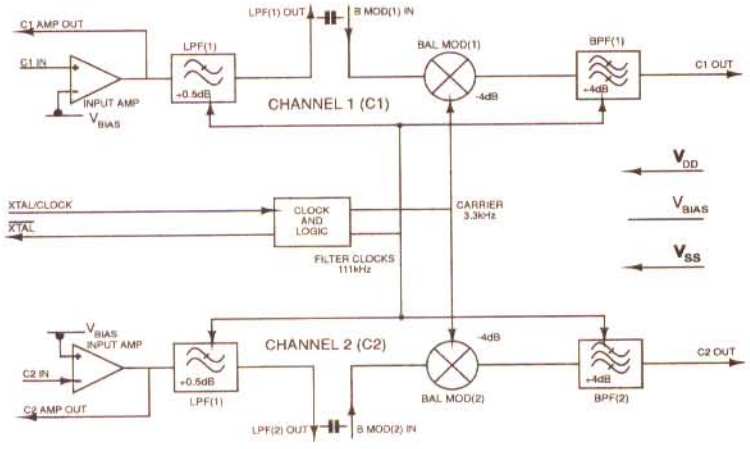
Wystarczy przez kilka minut przestrajać odbiornik w pasmach telefonii samochodowej, by zdać sobie sprawę z całkowitego braku jakiejkolwiek ochrony tajemnicy prowadzonych rozmów. Wielu użytkowników zdaje sobie sprawę z faktu, że ich najbardziej poufne rozmowy praktycznie odbywają się publicznie. Analogiczna jest sytuacja telefonii bezprzewodowej, jakkolwiek w tym przypadku zasięg jest ograniczony do najwyżej kilkuset metrów. W przypadku telefonii kablowej - nic prostszego jak podłączyć się do linii przy pomocy dwóch krokodylków.

Istnieje wiele możliwości technicznych zmodyfikowania wysyłanego dźwięku, czyli zaszyfrowania, tak by stał się niezrozumiały bez odpowiedniego zdekodowania. Szyfrowanie stosowane w łączności między centralą a aparatami ruchomymi oddaje znaczne usługi, a wymagania dotyczące pasma są niewielkie - kilka kanałów HF, tak więc urzędy zarządzające telekomunikacją zachęcają do jego stosowania. Niestety, szyfrowanie wiadomości przesyłanych w publicznej telekomunikacji utrudnia prowadzenie dochodzeń, i odpowiednie instytucje dążą do wprowadzenia zakazu szyfrowania rozmów.

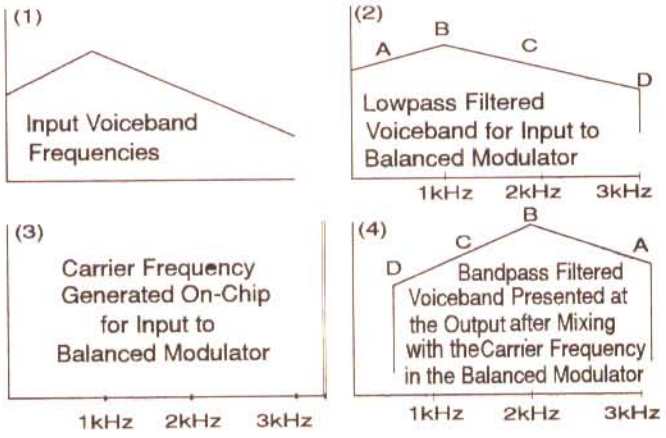
Dostępne do niedawna elementy elektroniczne do urządzeń szyfrujących były produkowane głównie na potrzeby wojska i podobnych instytucji, miały więc wysokie parametry, ale również i wysokie ceny.

Szybkiemu rozwojowi telefonii bezprzewodowej towarzyszy pojawienie się szyfrujących układów elektronicznych, o cenach wystarczająco atrakcyjnych z punktu widzenia elektroników-amatorów i dostatecznie wysokich parametrach z punktu widzenia instytucji zarządzających systemami telekomunikacyjnymi.

I tak np. Philips produkuje dwa oddzielne układy: szyfrujący i deszyfrujący, natomiast firma CML (Consumer Microcircuits Ltd.) produkuje układ FX118, zawierający obydwa



Rys. 1. Schemat blokowy układu FX118



Rys. 2. Widma sygnałów

bloki funkcjonalne. Właśnie ten ostatni układ został wybrany do zastosowania w opisywanym tutaj urządzeniu.

FX118 - układ szyfrujący z odwracaniem widma sygnału

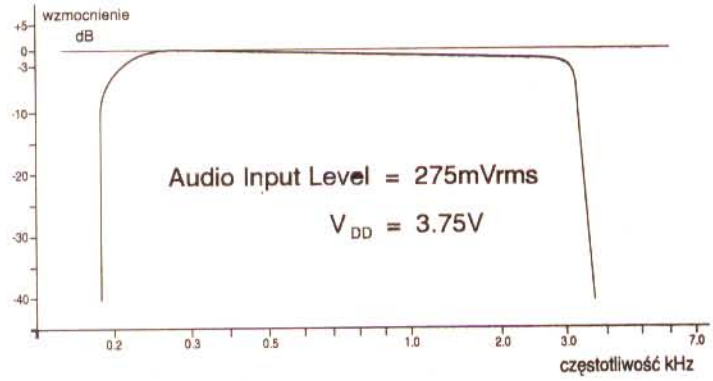
Układ FX118 wykorzystuje najprostszą z możliwych metodę szyfrowania - odwracanie widma sygnału. Nie jest to więc układ, którego zastosowanie uniemożliwi zdekodowanie informacji specjaliście pracującemu w odpowiednio wyposażonym laboratorium, niemniej jednak zniechęci przypadkowych świadków i poważnie utrudni zadanie okazjonalnemu detektywowi. Jest więc to rozwiązanie kompromisowe, dające w wielu wypadkach dobre rezultaty.

Schemat blokowy układu FX118 (**rys. 1**) zawiera dwa identyczne kanały przetwarzania informacji. Ponieważ szyfrowanie i deszyfrowanie są operacjami identycznymi, układ ten nadaje się szczególnie do rozwiązań typu „duplex". Odróżnia go to od stosowanych dotąd układów szyfrujących, pracujących zazwyczaj albo w trybie nadawania, albo odbioru, a więc niewygodnych w zastosowaniu w telefonii.

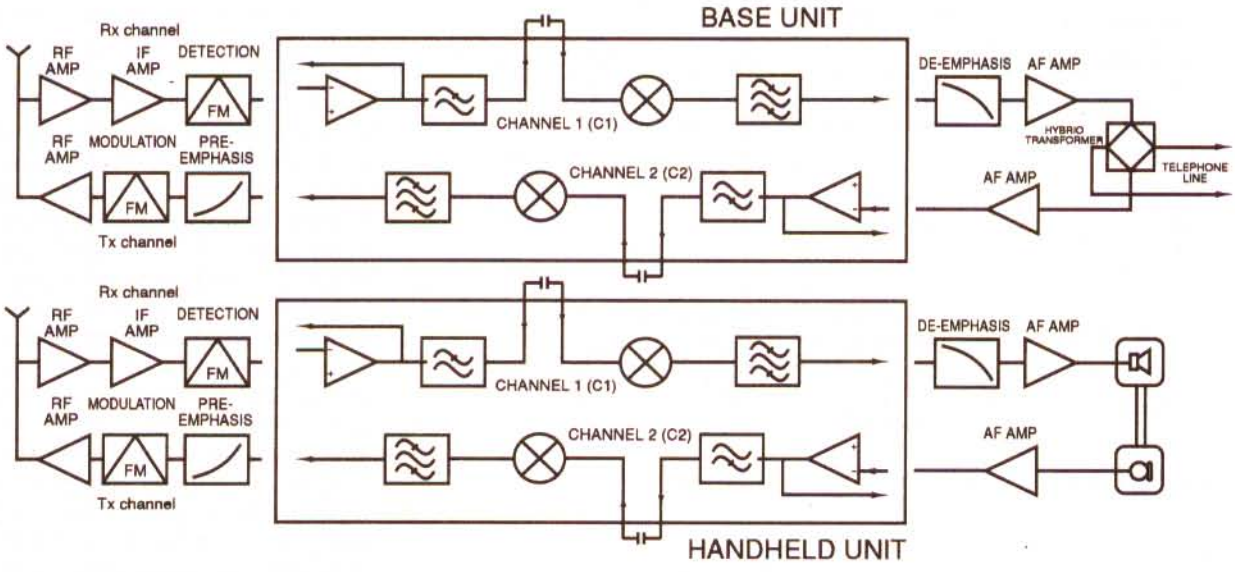
Widma sygnałów przedstawione na **rys. 2** prezentują zasadę szyfrowania. Sygnał mowy o pasmie ograniczonym do 3kHz przez filtr dolnoprzepustowy odpowiednio wysokiego rzędu jest podawany na modulator zrównoważony, wraz z sygnałem fali nośnej o częstotliwości 3300Hz, uzyskanej z podziału częstotliwości generatora kwarcowego. W wyniku modulacji uzyskuje się dwa sygnały. Widmo jednego z nich, leżące powyżej 3300Hz, o częstotliwościach będących sumą częstotliwości sygnałów wejściowych modulatora, jest łatwe do eliminacji drogą filtracji. Widmo drugiego sygnału, leżące poniżej 3300Hz, ma rozkład obrócony wokół częstotliwości 1650Hz w stosunku do sygnału szyfrowanego, np. wartość widmowej gęstości mocy odpowiadająca częstotliwości 500Hz w sygnale pierwotnym staje się wartością odpowiadającą częstotliwości 2800Hz w sygnale zaszyfrowanym.

Zaszyfrowana w ten sposób rozmowa staje się niezrozumiała, a sygnał zajmuje dokładnie taką samą szerokość pasma jak przed zaszyfrowaniem i może być przesyłany w tym samym systemie.

Oczywiście, analogiczna operacja modulacji, przeprowadzona na sygnale zaszyfrowanym, umożliwia zdeszyfrowanie informacji, pod warunkiem spełnienia przez oba urządzenia dwóch warunków. Po pierwsze, generatory lokalne urządzenia szyfrującego i deszyfrującego muszą być dostrojone dokładnie do tej samej częstotliwości, co jest stosunkowo łatwe w realizacji pod warunkiem zastosowania generatorów kwarcowych. Po drugie, należy wyeliminować z widma sygnału podawanego na modulator urządzenia szyfrującego wszelkie składowe równe lub leżące powyżej częstotliwości nośnej oraz składowe widma sumarycznego (powyżej częstotliwości nośnej)



Rys. 3. Charakterystyka amplitudowo-częstotliwościowa układu szyfrującego



Rys. 4. Tor transmisji z układem FX118

w sygnale wyjściowym modulatora. Wymaga to zastosowania nie tylko bardzo wysokiej jakości modulatora, ale także filtrów aktywnych odpowiednio wysokiego rzędu (10...15). Realizacja takich układów na wzmacniaczach operacyjnych byłaby raczej trudna.

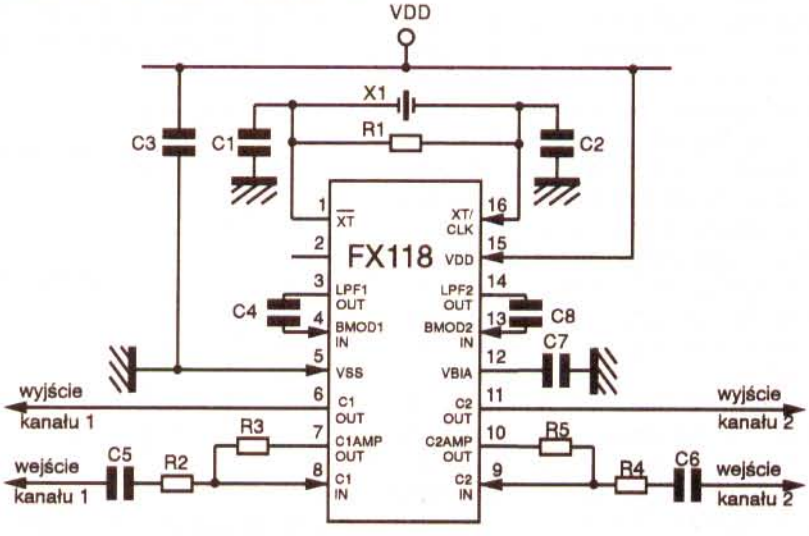
Firma CML specjalizuje się w filtrach przełączanych, np. produkowane przez nią detektory częstotliwości (tonu) stosowane w systemach selektywnego wywoływania, uważane są za jedne z najlepszych. Wejściowy filtr dolnoprzepustowy 10-go rzędu układu FX118 wprowadza tłumienie 3dB dla 3100Hz i 30dB dla 3300Hz. Wyjściowy filtr pasmowo przepustowy 14-go rzędu wprowadza tłumienie 48dB dla 3400Hz, zaś nachylenie jego charakterystyki amplitudowej poniżej 250Hz wynosi 18dB na oktawę. Wypadkowa charakterystyka amplitudowa układu szyfrującego lub deszyfrującego (**rys. 3**), o pasmie 200...3000Hz, doskonale nadaje się do zastosowań w telefonii kablowej i radiowej. Dodatkowym elementem ułatwiającym realizację urządzenia jest wejściowy wzmacniacz o regulowanym wzmocnieniu, znajdujący się w każdym torze układu FX118.

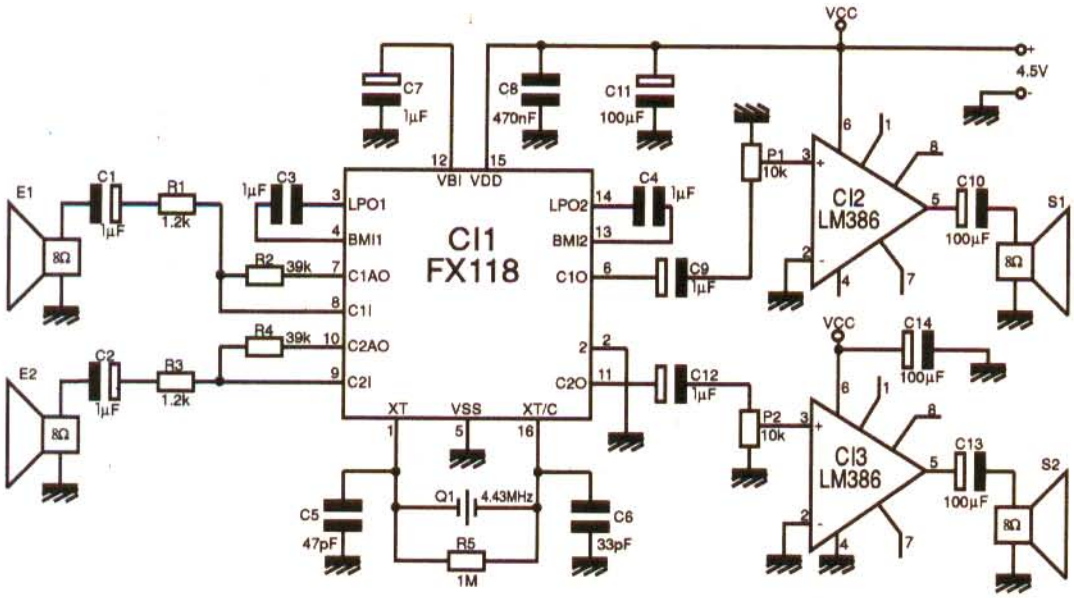
Urządzenie szyfrująco-deszyfrujące

Zaprojektowany z myślą o zastosowaniach w telefonii samochodowej, układ FX118 jest zazwyczaj umieszczany w torze transmisji centrali i aparatu ruchomego (**rys. 4**). Prezentowane tu urządzenie jest bardziej uniwersalne, ponieważ może współpracować z dowolnym aparatem telefonicznym, poprzez sprzężenie akustyczne. Można je więc (z uwzględnieniem odpowiednich przepisów prawnych) stosować w telefonie domowym, publicznym, samochodowym, w morskiej łączności radiowej czy wreszcie w telefonii prywatnej. Wymaga to uzupełnienia schematu przedstawionego na **rys. 5** o wzmacniacze mocy, z których jeden wysterowuje niewielki głośnik umieszczony naprzeciw mikrofonu słuchawki, a drugi wzmacnia sygnał odbierany. Wspólny generator obu części funcjonalnych układu FX118 powinien pracować z kwarcem o częstotliwości rezonansowej 4,43MHz. Możliwe jest także użycie kwarców o innych częstotliwościach rezonansu, np. 3,58MHz, co spowoduje jednak pewne zmiany parametrów całego systemu. Ponieważ istnieje możliwość zniszczenia układu FX118, jeśli zostanie zasilony bez podłączonego kwarcu, lub jeśli jego generator nie działa, na etapie uruchamiania układu zalecane jest stosowanie zasilaczy z ograniczaniem prądu.

Ponieważ wzmocnienie przedwzmacniaczy układu FX118 jest wysokie, jako mikrofonów można użyć niewielkich głośników 8Ω/5cm, z których jeden zostanie umieszczony przed słuchawką, drugi zaś - przed ustami mówiącego. W ten oto sposób dochodzimy do ostatecznego schematu (**rys.6**), który uzupełnić można jedynie o baterię płaską

Rys. 5. Schemat aplikacyjny układu FX118





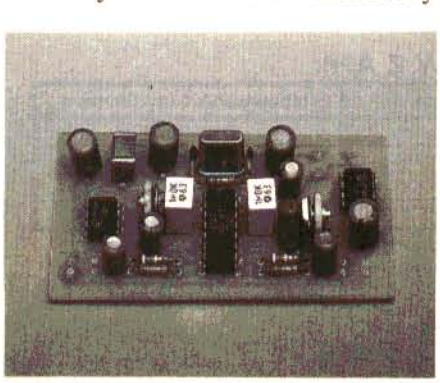
Rys. 6. Schemat elektryczny urządzenia

4.5V lub trzy baterie AA połączone szeregowo (układ FX118 może być zasilony napięciem 3...5.5V).

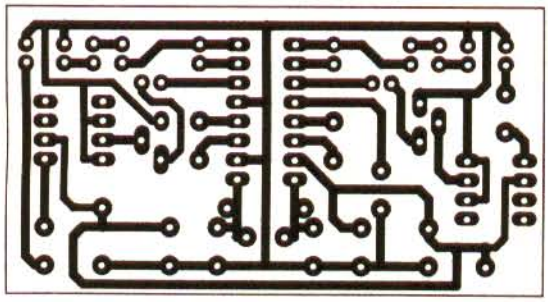
Mozaikę ścieżek płytki i rozmieszczenie elementów przedstawiają **rysunki 7 i 8**. Płytkę, z racji niewielkich rozmiarów, można będzie umieścić w słuchawce aparatu telefonicznego lub innej obudowie, zapewniającej sprzężenie akustyczne z mikrofonem telefonu.

Do pierwszych prób wystarczy wykonać jeden egzemplarz urządzenia, co pozwoli sprawdzić, czy głośniki S1 i S2 emitują wyłącznie niezrozumiałe dźwięki, jeśli mówi się do E1 i E2. Następnie należy umieścić S1 przed E2, wyregulować wzmocnienia w sposób pozwalający na uniknięcie wzbudzeń, po czym mówić do E1. Dźwięk w głośniku S2 powinien być niezrozumiały, z dopuszczalnym niewielkim szumem.

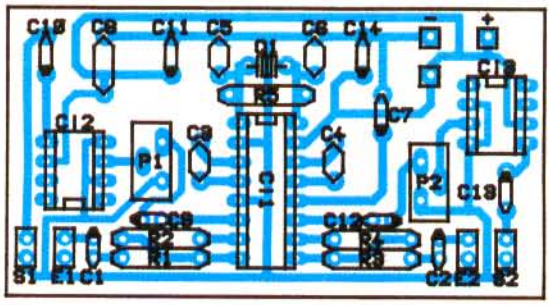
Po wykonaniu drugiego egzemplarza należy zestawić system według **rys.9**. Podstawowa regulacja, której należy dokonać, dotyczy wzmocnienia wszystkich czterech wzmacniaczy mocy. Zależnie od czułości głośników użytych w miejsce mikrofonów (lub mikrofonów, jeśli ktoś wybierze takie rozwiązanie) może okazać się konieczna zmiana rezystorów 39kΩ ustalających wzmocnienia poszczególnych przedwzmacniaczy. Należy pamiętać o tym, że zbyt małe wzmocnienie sygnału mikrofonu, skompensowane nadmiernym wzmocnieniem wzmacniacza mocy, może spowodować znaczny spadek stosunku sygnału do szumu.



Rys. 7. Mozaika ścieżek płytki drukowanej



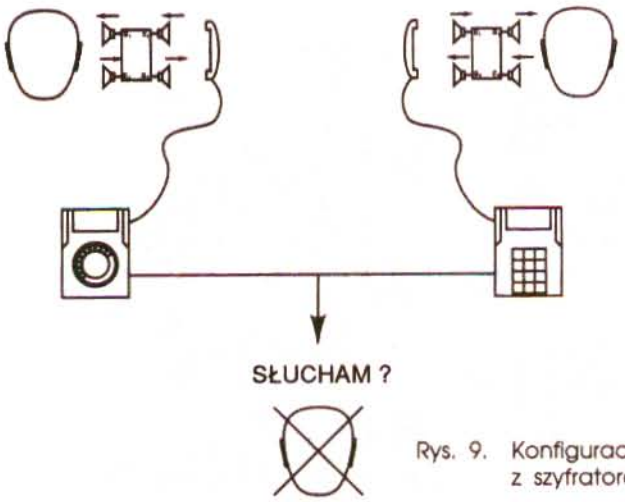
Rys. 8. Rozmieszczenie elementów na płytce drukowanej



Tor układu FX118 (bez przedwzmacniaczy) pracuje z sygnałami o wartości skutecznej około 400mV.

Zakończenie

Zastosowanie szyfrowania jest w pełni dozwolone (a nawet czasem zalecane) w telefonii bezprzewodowej, nie jest natomiast dozwolone w publicznej sieci telefonicznej. Tymczasem użytkownik telefonu ma prawo do ochrony tajemnicy swych rozmów, które w najmniejszym na-



Rys. 9. Konfiguracja linii telefonicznej z szyfratorem

wet stopniu nie jest zapewnione w przypadku telefonii samochodowej. Zastanawiające jest jak - przy powszechnej dostępności sprzętu umożliwiającego podsłuchiwanie rozmów telefonicznych - można zabraniać stosowania przez uczciwych obywateli środków mających chronić ich życie prywatne!

Patrick Guelle, ERP

WYKAZ ELEMENTÓW

Rezystory

R1, R3: 1.2kΩ
R2, R4: 39kΩ
R5: 1MΩ
P1, P2: 10kΩ

Kondensatory

C1 - C4, C7, C9, C12: 1µF
C5: 47pF
C6: 33pF
C8: 470nF
C10, C11, C13, C14: 100µF

Układy scalone

CI1: FX118
CI2, CI3: LM386

Różne

S1, E1, S2, E2: głośniki 8Ω
Q1: kwarc 4,43MHz