

```
#include <stdint.h>
#include <stdlib.h>
#include <string.h>
#include <stdio.h>

// Write 12+ptlen bytes to ct (ciphertext preceded by 12 byte random nonce)
void chat_encrypt(void *k, void *pt, int ptlen, void *ct);

// Write ctlen-12 bytes to pt (using the first 12 bytes of ct as the nonce)
void chat_decrypt(void *k, void *ct, int ctlen, void *pt);

int main() {
    unsigned char k[32];
    unsigned char pt[100];
    unsigned char ct[112];
    chat_encrypt(k, pt, 100, ct);
    chat_decrypt(k, ct, 112, pt);
    return 0;
}
```