

# Netzwerksicherheit

## Übung 3

Tobias Limmer

Computer Networks and Communication Systems  
Dept. of Computer Sciences, University of Erlangen-Nuremberg, Germany

19. – 23.11.2007

# Besprechung der Hausaufgabe

# Besprechung der Hausaufgabe

## Originalnachricht

UKW: B

W/O: B241

Stecker: ATBLDFGJHMNWOPQYZVX

Rings: AAV

Message key: VJNA

vonvonjlooksjhffttteinseinsdreizwoyyqnsneuninhalt  
xxbeiangriffunterwassergedruecktywabosxletztergegn  
erstandnulachtdreinuluhrrmarquantonjotaneunachtseyh  
sdreiyzwozwonulgradyachtsmystossenachxeknsviermbfa  
elltynnnnnnoovierysichteinsnull

# Besprechung der Hausaufgabe

## Interpretation

Von Looks:

Funktelegramm 1132/19 Inhalt:

Bei Angriff unter Wasser gedruickt, Wasserbomben.  
Letzter Gegnerstandort 08:30 Uhr, Marqu AJ 9863,  
220 Grad, 8 Seemeilen, stosse nach. 14 Millibar  
faellt, NNO 4, Sicht 10.

# RSA

- Erweiterter Euklidischer Algorithmus:

$$d = \gcd(a, b) = m \times a + n \times b$$

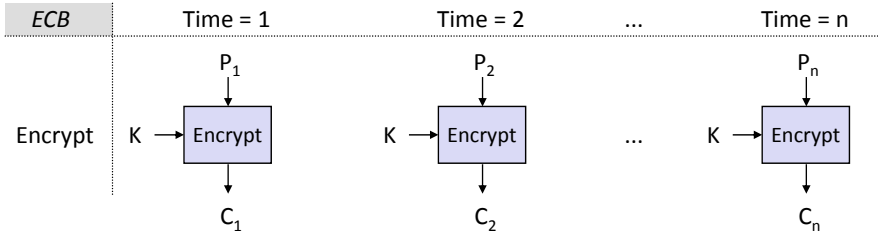
## Algorithmus:

```
(int d, m, n) = ExtendedEuclid(int a, b)
{
    if (b=0) return (a, 1, 0);

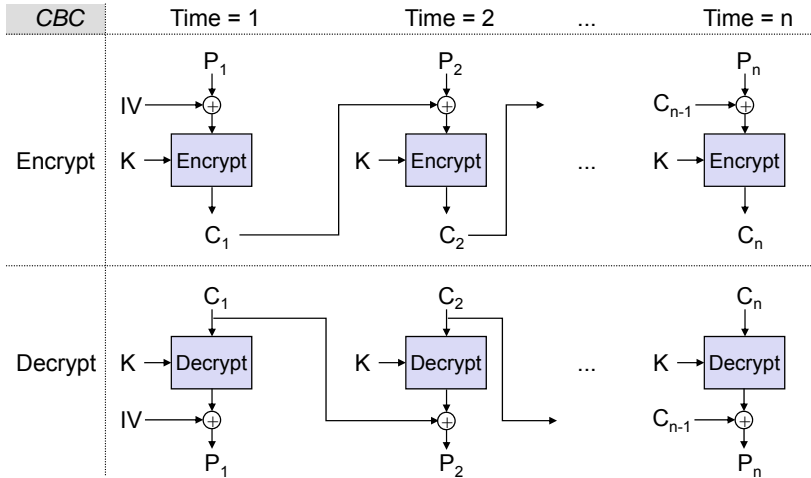
    (d', m', n') = ExtendedEuclid(b, a mod b);
    (d, m, n) = (d', n', m'-RoundDown(a/b)*n');

    return (d, m, n);
}
```

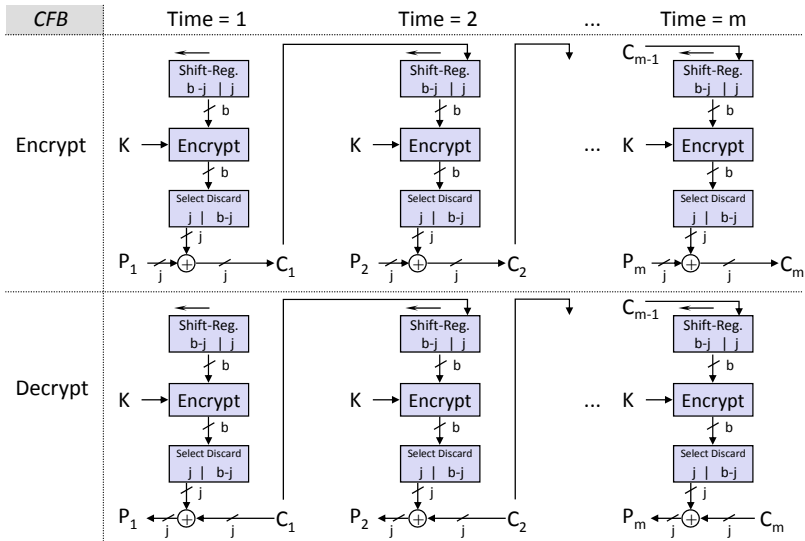
# Betriebsmodus ECB (Electronic Code Book)



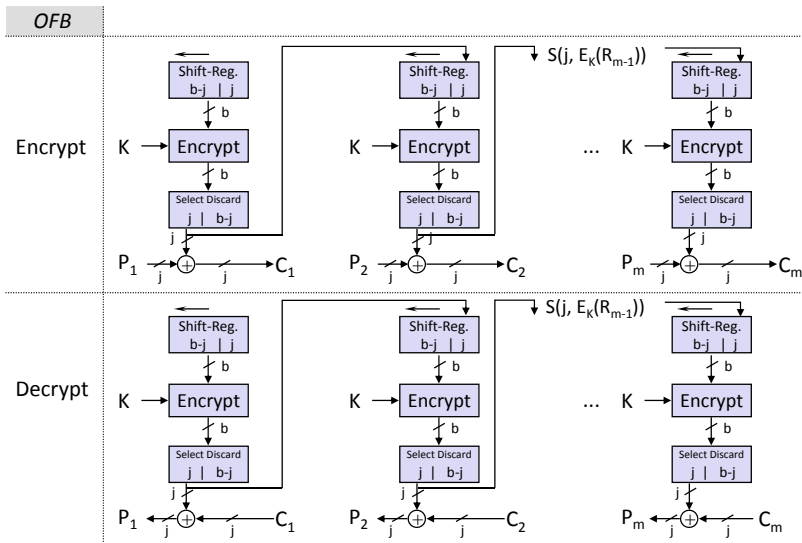
# Betriebsmodus CBC (Cipher Block Chaining)



# Betriebsmodus CFB (Ciphertext Feedback)



# Betriebsmodus OFB (Output Feedback)



# Übungsaufgabe

- DES wird über folgende Funktion verwendet:

```
void netsec_des_crypt(int mode, const_DES_cblock *input,  
                      DES_cblock *output, char *key);
```

- Parameter `mode` gibt an, ob ver- oder entschlüsselt werden soll
- es werden immer 8-Byte Blöcke bearbeitet
- Parameter `key` ist null-terminierter String

## Deklarationen

```
typedef unsigned char DES_cblock[8];  
typedef /* const */ unsigned char const_DES_cblock[8];
```

# Übungsaufgabe

- **Achtung:** Bei Kompilierung/Linkvorgang des Programms muss die OpenSSL-Bibliothek eingebunden werden. Dazu muss `gcc` der Parameter `-lssl` übergeben werden.