Caeser Cipher

Stockholm University

Cleartext: `Maggie, Thursday, 7pm.`

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

Caeser Cipher

Stockholm University

Cleartext: Maggie, Thursday, 7pm.

ABCDEFGHIJKLMNOPQRSTUVWXYZ

DEFGHIJKLMNOPQRSTUVWXYZABC

Pdjjlh, Wkxuvgdb, 7sp.

Letter frequencies in English text†

Stockholm University

	%		%		%
E	**13.1**	**D**	**4.1**	**G**	**1.4**
T	**9.0**	**L**	**3.6**	**B**	**1.3**
O	**8.2**	**C**	**2.9**	**V**	**1.0**
A	**7.8**	**F**	**2.9**	**K**	**0.4**
N	**7.3**	**U**	**2.8**	**X**	**0.3**
I	**6.8**	**M**	**2.6**	**J**	**0.2**
R	**6.6**	**P**	**2.2**	**Q**	**0.1**
S	**6.5**	**Y**	**1.5**	**Z**	**0.1**
H	**5.9**	**W**	**1.5**		

†Davies, D.W. & Price, W.L., "*Security for Computer Networks*", Wiley, 1989

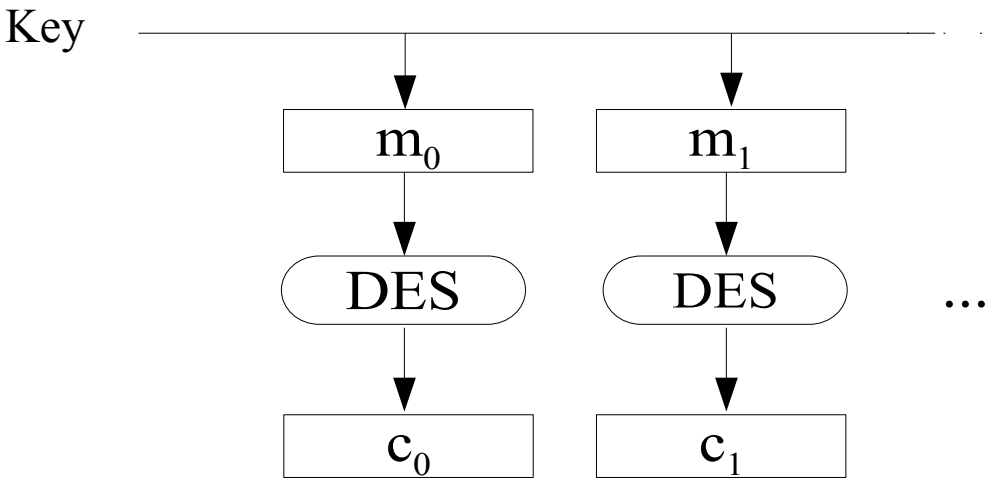
Digrams and trigrams in English text†

TH	THE
HE	AND
AN	THA
IN	ENT
ER	ION
RE	TIO
ES	FOR
ON	NDE
EA	HAS
TI	NCE

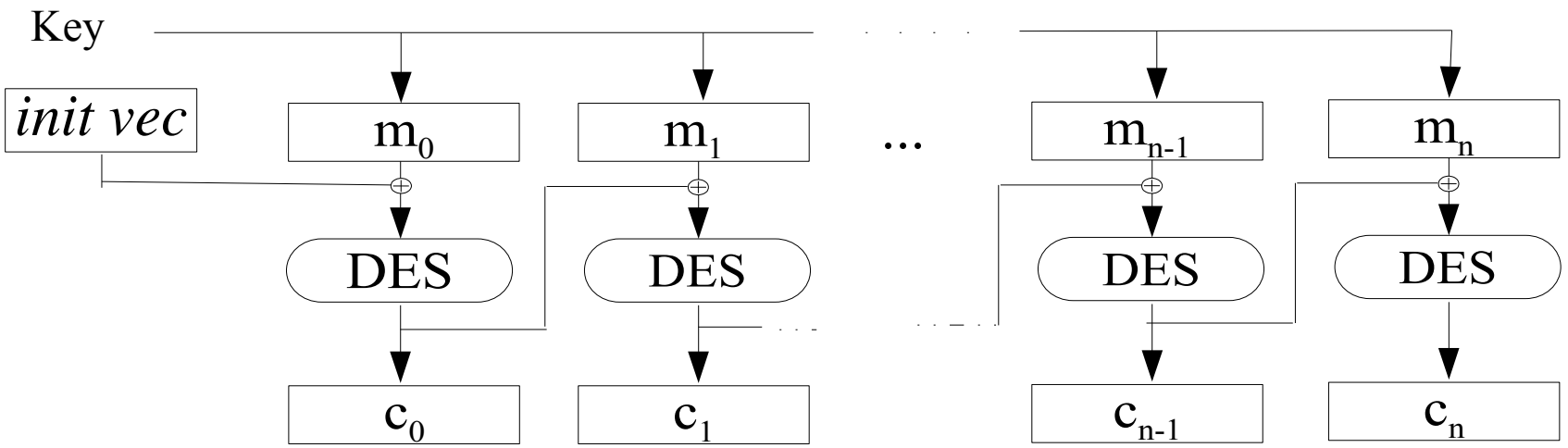
†Davies, D.W. & Price, W.L., "*Security for Computer Networks*", Wiley, 1989

DES Encryption

Stockholm University



DES CBC Mode



RSA

c = cryptotext
m = message
public key = (e,n)
private key = d

- $c = m^e \bmod n$
- $m = c^d \bmod n$