

Kryptologi

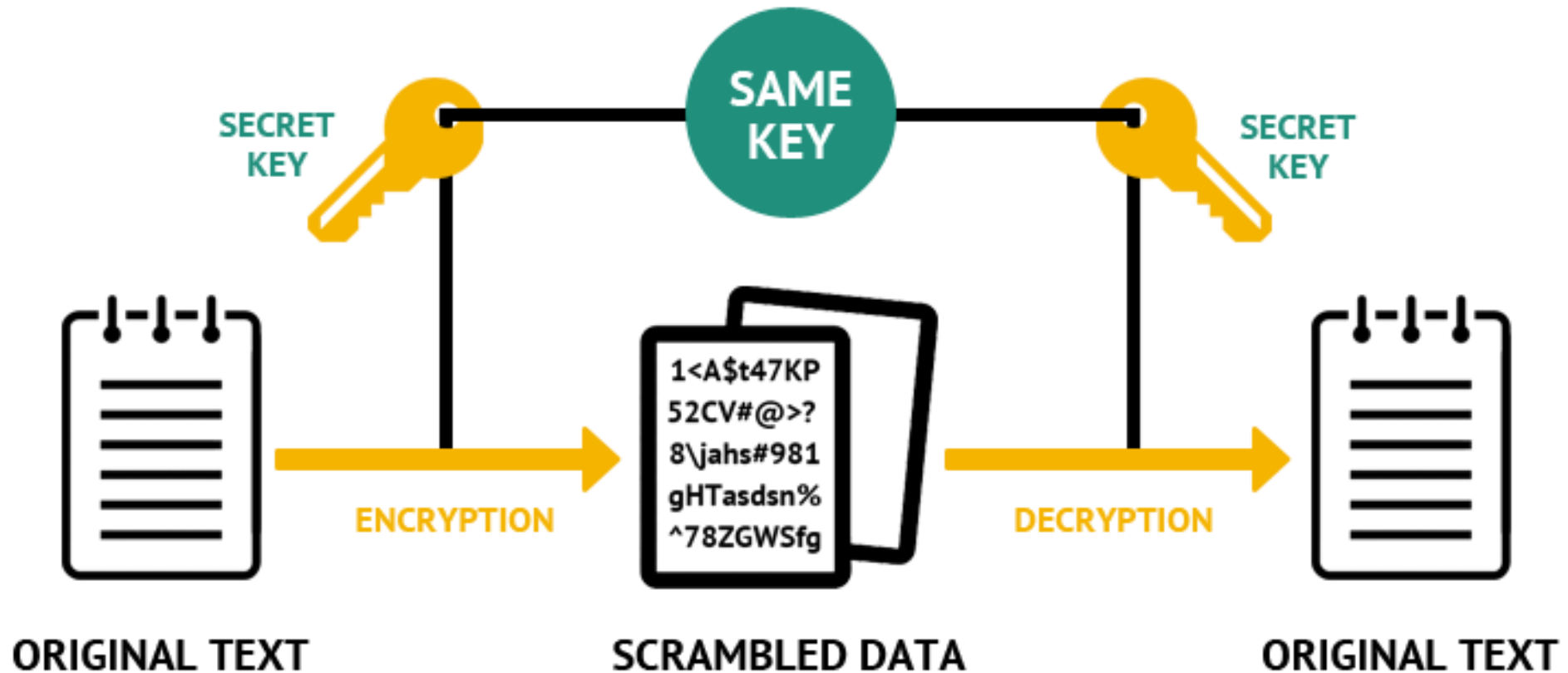


Kryptologi

- Læren om hemmeligholdelse af information (fra græsk):
 - kryptos: hemmelig
 - -logi: læren om

Idéen er altså...

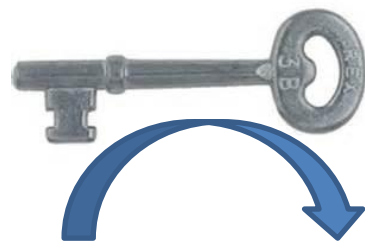
Symmetric Encryption



Eksempel - afsender

Klartekst

ANGRIB VED
DAGGRY



Kryptotekst

IVOZQJ AML
LIOOZD

Eksempel - modtager

Kryptotekst

IVOZQJ AML
LIOOZD



Klartekst

ANGRIB VED
DAGGRY

Cæsar substitution

- en simpel form for Monoalfabetisk substitution (et additiv kryptosystem)
- "one digit encryption"

- Alle bogstaver i alfabetet flyttes et antal pladser frem (f.eks. 3 – det er nøglen!)

Klar- tekst	A	B	C	D	E	F	G	H	I
Krypto- tekst	D	E	F	G	H	I	J	K	L

- Hvordan skriver man DAGE?

Øvelse – cæsar substitution

- a) Vælg en nøgle som du vil bruge til at lave "1 digit encryption" (dvs. et tal mellem 1 og 28)
- b) Skriv en *kort tekst* (tre små ord) til din sidemand
- c) Krypter din tekst
- d) Send din tekst til sidemanden og angiv din nøgle
- e) Lad din sidemand dekryptere din tekst

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Æ	Ø	Å
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Overvej: Hvor mange forskellige nøgler er der? Er det nemt at bryde dette kryptosystem?

MULTI DIGIT ENCRYPTION

- Nøgle: 5 3 7 8 ("4 digit encryption")

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

- Hvordan skriver man DAGE?
- Dette er et eksempel på symmetrisk kryptering – hvorfor?
- Hvorfor er det ikke smart på internettet?

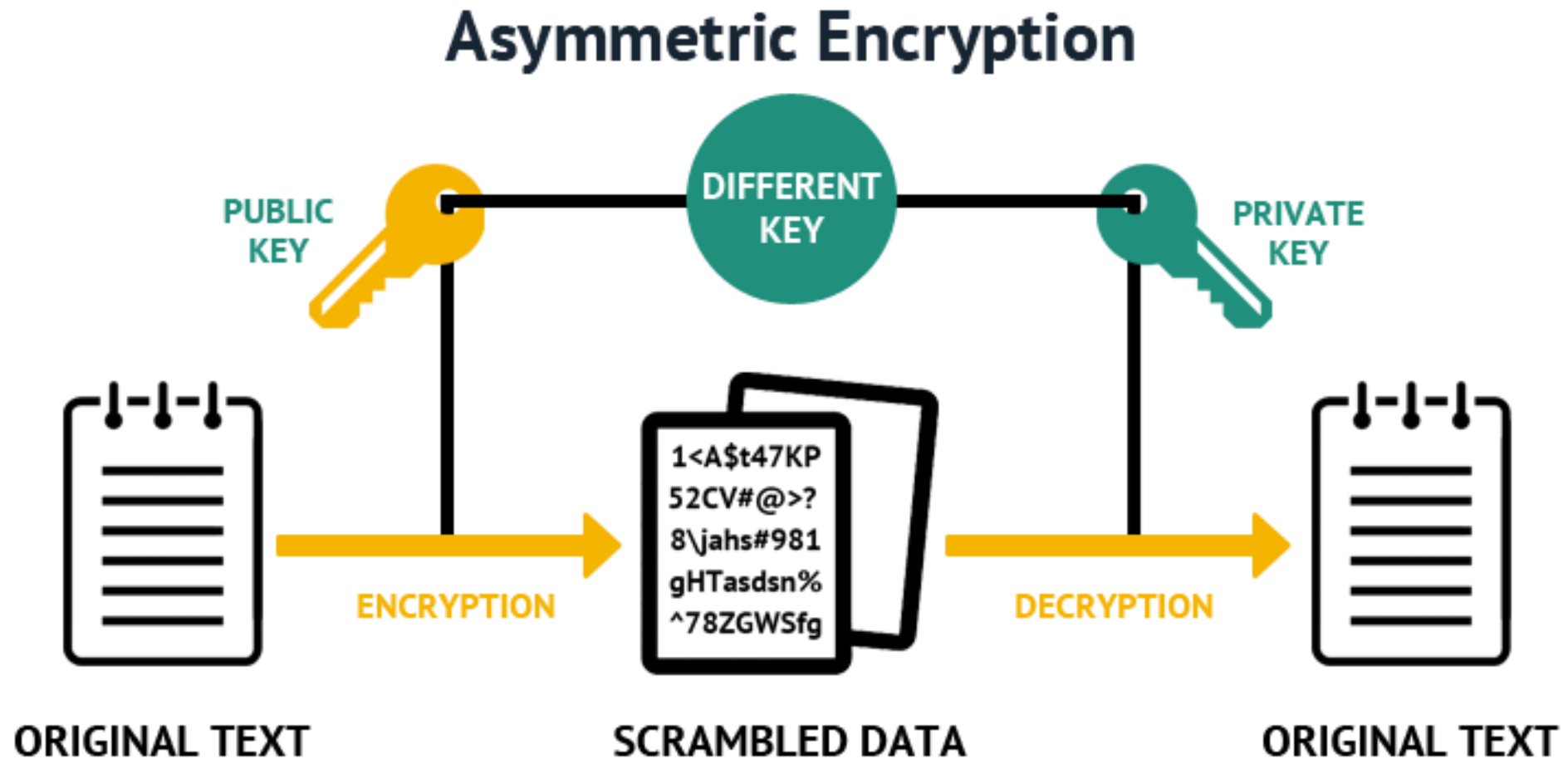
Øvelse – MULTI DIGIT ENCRYPTION

- a) Vælg en nøgle på 3 cifre som du vil bruge til at lave "multi digit encryption"
- b) Skriv en *et ord* til din sidemand
- c) Krypter din tekst
- d) Send din tekst til sidemanden og angiv din nøgle
- e) Lad din sidemand dekryptere din tekst

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Æ	Ø	Å
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

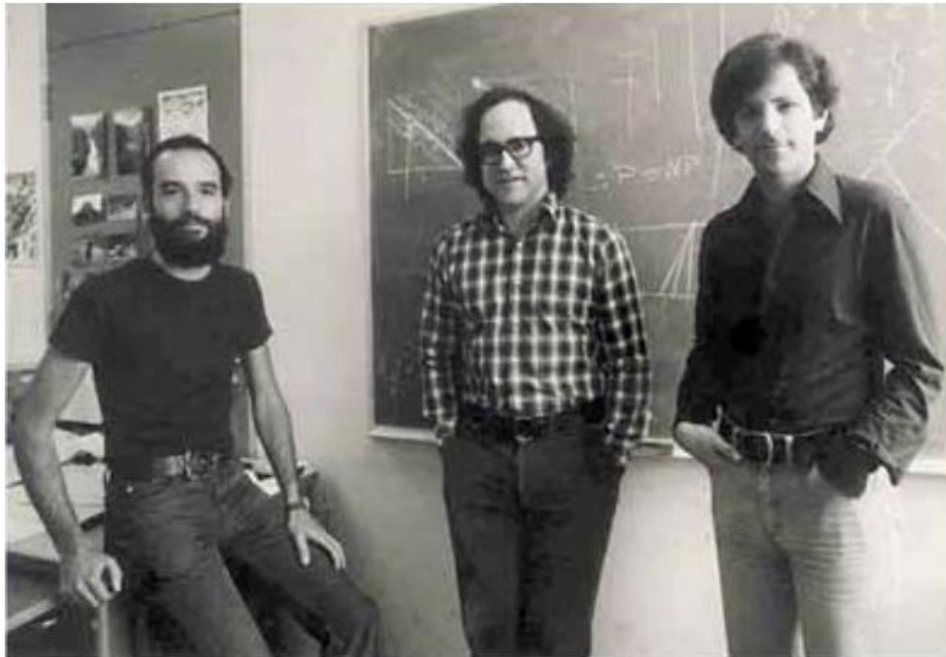
Overvej: Hvor mange forskellige nøgler er der? Er det nemt at bryde dette kryptosystem?

Asymmetrisk kryptering



Asymmetrisk kryptering: RSA kryptering

- Rivest, Shamir og Adleman (1977)



Adi Shamir (1952-), Ronald Rivest (1948-) og Leonard Adleman (1945-).

Modulo regning
– dvs. regning med rester

Hvad er resten, hvis 25 divideres med 7?

Da

$$25 = 7 \cdot 3 + 4$$

så er resten 4.

Det skriver man sådan her:

$$25 \bmod 7 = 4$$

Asymmetrisk kryptering: RSA kryptering

Generelt

- Vælg to primtal p og q
- Udregn $n = p \cdot q$ og $z = (p - 1) \cdot (q - 1)$
- Vælg e sådan at e og z ikke har nogle faktorer til fælles (udover 1).
- Vælg d sådan at z går op i $e \cdot d - 1$

Eksempel

- $p = 3$ og $q = 5$
- $n = 3 \cdot 5 = 15$ og $z = 2 \cdot 4 = 8$
- Vi vælger $e = 11$ ($z = 8 = 2 \cdot 2 \cdot 2$ og e er et primtal – altså ingen faktorer til fælles).
- Vi har her $z = 8$ og $e \cdot d - 1 = 11 \cdot d - 1$. Vi prøver os frem:

d	$11 \cdot d - 1$
1	10
2	21
3	32

BINGO!



Asymmetrisk kryptering: RSA kryptering

Public key: (15,11)
Private key: (15,3)

Generelt

- Vælg to primtal p og q
- Udregn $n = p \cdot q$ og $z = (p - 1) \cdot (q - 1)$
- Vælg e sådan at e og z ikke har nogle faktorer tilfælles (udover 1).
- Vælg d sådan at z går op i $e \cdot d - 1$

Public key: (n, e)
Private key: (n, d)

Eksempel

- $p = 3$ og $q = 5$
- $n = 3 \cdot 5 = 15$ og $z = 2 \cdot 4 = 8$
- Vi vælger $e = 11$ ($z = 8 = 2 \cdot 2 \cdot 2$ og e er et primtal – altså ingen faktorer tilfælles).
- Vi har her $z = 8$ og $e \cdot d - 1 = 11 \cdot d - 1$. Vi prøver os frem:

d	$11 \cdot d - 1$
1	10
2	21
3	32

BINGO!

Asymmetrisk kryptering: RSA kryptering

Generelt

- Til kryptering af beskeden $m < n$ bruges den offentlige nøgle (n, e) .
- Kryptoteksten c er da:
$$c = m^e \bmod n$$
- Man dekrypterer ved at bruge den private nøgle (n, d) :
$$c^d \bmod n = m !!!$$

Eksempel

- Vi vil kryptere $m = 13 < 15$ med den offentlige nøgle $(15, 11)$.
- Kryptoteksten er:
$$c = 13^{11} \bmod 15 = 7$$
- Man dekrypterer ved at bruge den private nøgle $(15, 3)$:
$$7^3 \bmod 15 = 13 !!$$

Asymmetrisk kryptering: RSA kryptering

- Sikkerheden består i, at det er svært (som i: det tager *sygt* lang tid) at defaktorisere

$$n = p \cdot q$$

hvis de to primtal er tilstrækkeligt store!

Asymmetrisk kryptering: RSA kryptering

- Hvis jeg vil sende beskeden: INFORMATIK så gør jeg sådan her...

-	→	00	F	→	06	L	→	12	R	→	18	X	→	24
A	→	01	G	→	07	M	→	13	S	→	19	Y	→	25
B	→	02	H	→	08	N	→	14	T	→	20	Z	→	26
C	→	03	I	→	09	O	→	15	U	→	21	Æ	→	27
D	→	04	J	→	10	P	→	16	V	→	22	Ø	→	28
E	→	05	K	→	11	Q	→	17	W	→	23	Å	→	29

INFORMATIK = 09 14 06 15 18 13 01 20 09 11

914 615 1813 120 911

Dvs. at vi her
har brug for
 $n > 1813$

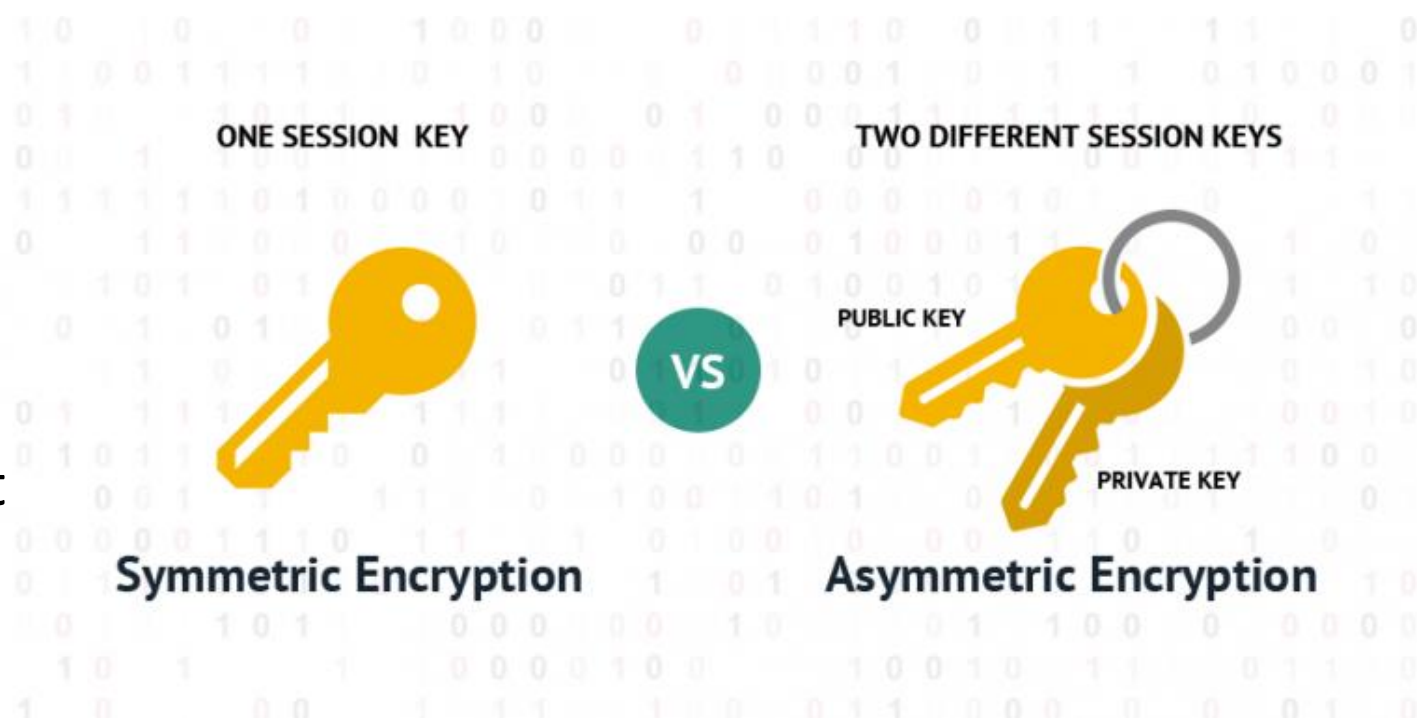
Hvorfor laver man blokke i stedet for at tage ét bogstav ad gangen?

Kryptering versus cookies

- Protokollerne SSL eller TLS sørger for at de data, som udveksles mellem klient og server, er krypterede – altså en sikker forbindelse.
- Men protokollerne har intet med cookies at gøre – cookies kan stadig gemmes på klientens computer.

Kryptering på internettet

- Asymmetrisk kryptering bruges til at udveksle en hemmelig nøgle
- Herefter bruges denne nøgle til symmetrisk kryptering (fordi det er hurtigere)
- Asymmetrisk kryptering bruges også til digitale signaturer



Skriv i din logbog (overskrift: "Encryption and public keys")

- Forklar kort MED DINE EGNE ORD!
 - Hvad går Cæsar substitution ud på? Hvorfor anvendes denne krypteringsmetode ikke længere?
 - Hvad går "multi digit encryption" ud på? Og hvorfor er det smartere end Cæsar substitution (som svarer til "one digit encryption")?
 - Hvad er forskellen på symmetrisk og asymmetrisk kryptering?
 - Hvorfor bruger man ikke alene symmetrisk kryptering, når man skal sikre trafikken på internettet? Hvad bruges i stedet?