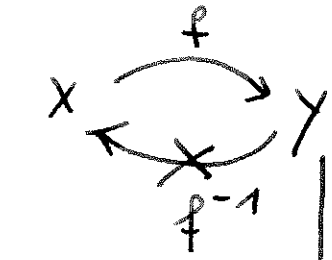
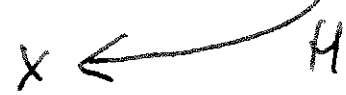
Zusammenfassung von letzter Vorlesung:

Einweg-fkt:



$\exists$ (geheimes Schlüssel)
Hintertürchen (trapdoor)



zyklische Gruppe: $G = \{a^1, a^2, a^3, \ldots, a^{|G|}\}$

wobei $|G| = \varphi(n)$ sofern

$G = \mathbb{Z}_n^*$ und

$|G| = n-1$ sofern

$G = \mathbb{Z}_n^*$, n Primzahl.

$U \subseteq G$, Untergruppe $\Rightarrow$ $|U|$ teilt $|G|$.

$\langle a \rangle = \{a^0, a^1, a^2, \ldots\}$ ist Untergruppe von G.

$a \in G$

Ordnung von $a \in G$ ist kleinstes $i > 0$ so dass

$$a^i = 1$$

$x \cdot y = 1$ bedeutet x, y invers zueinander

$y^2 = x$ bedeutet x ist Quadratzahl, y ist Quadratwurzel von x.

Wenn G eine zyklische endliche Gruppe ist, so gilt für ein $a \in G$, dass

$$a^1, a^2, a^3, \ldots, a^{|G|}$$

alle Gruppenelemente durchläuft. Danach, also ab $a^{|G|+1}$ fängt die Folge wieder bei a^1 an.
Andernfalls hätten wir:

$$a^1 \to \cdots \to a^i \to \cdots \to a^{|G|}$$

Dann hätte a^i die 2 verschiedenen Vorgänger a^{i-1} und $a^{|G|}$. Das geht nicht, sonst würde gelten: $a^{i-1} \neq a^{|G|}$ und $a \cdot a^{i-1} = a a^{|G|}$.

Da $a^{|G|}$ Vorgänger von a^1 ist, ist $a^{|G|} = a^0 = 1$.

Auch in dem Fall, wenn a eine kleinere Ordnung als die Gruppenordnung hat, sagen wir j, dann ist $\{a^1, a^2, \ldots, \underbrace{a^j}_{=1}\}$ eine Untergruppe von G, und damit ist j ein Teiler von $|G|$. Damit ist auch für ein solches a:

$$a^1 a^2 \ldots \underbrace{a^j}_{=1} a^{j+1} \ldots \underbrace{a^{2j}}_{=1} \ldots \underbrace{a^{|G|}}_{=1}$$

Satz von Euler: Für jede endliche Gruppe G und jedes Gruppenelement $a \in G$ ist

$$a^{|G|} = 1 \quad \text{(das neutrale Element von } G\text{)}.$$

Im Kontext von $G = \mathbb{Z}_n^*$ heißt das:

$$a^{\varphi(n)} \equiv 1 \pmod{n} \quad \text{für alle } a \in \mathbb{Z}_n^*.$$

Im Spezialfall, dass n Primzahl ist, heißt das:

("Kleiner Satz von Fermat"):

$$a^{n-1} \equiv 1 \pmod{n} \quad \text{für alle } a \in \mathbb{Z}_n^*.$$

Wir haben mit diesen Überlegungen auch ein Kriterium dafür, ob a ein Erzeuger der Gruppe G ist (ohne dafür alle a^i berechnen zu müssen):

Für alle Primteiler p von $|G|$ muss gelten:

$$a^{|G|/p} \neq 1$$

Im Kontext von $G = \mathbb{Z}_n^*$, n Primzahl, heißt, dass gelten muss: $a^{(n-1)/p} \not\equiv 1 \pmod{n}$ für alle Primteiler von $n-1$. (Dies setzt voraus, dass man die Faktorisierung von $n-1$ kennt.)

Betrachten wir eine zyklische Gruppe $\mathbb{Z}_n^*$.

D.h. für ein $a \in \mathbb{Z}_n^*$ gilt:

$$\mathbb{Z}_n^* = \{a^1, a^2, \dots, a^{\varphi(n)}\}$$

Die a's wiederholen sich zyklisch, also:

$$a^i \equiv a^{i+\varphi(n)} \equiv a^{i+2\cdot\varphi(n)} \dots \pmod{n}$$

Aus dieser Beobachtung ergibt sich der folgende

Satz: Sei $\mathbb{Z}_n^*$ eine zyklische Gruppe und $a \in \mathbb{Z}_n^*$ eine Primitivwurzel mod n. Dann gilt:

$$a^x \equiv a^y \pmod{n} \iff x \equiv y \pmod{\varphi(n)}$$

Falls $\mathbb{Z}_n^*$ nicht zyklisch ist, oder falls a keine Primitivwurzel ist, und somit eine Ordnung besitzt, die Teiler von $\varphi(n)$ ist, so gilt im obigen Satz zumindestens die Richtung von rechts nach links ($\Leftarrow$).

Eine weitere Konsequenz der Betrachtungen.

Seien x und x' zueinander invers, modulo $\varphi(n)$.

Also $x \cdot x' \equiv 1 \pmod{\varphi(n)}$.

D.h. $x \cdot x' = 1 + k \cdot \varphi(n)$ für ein $k \in \mathbb{Z}$.

Dann folgt $(m^x)^{x'} \pmod n$ (sei $m \in \mathbb{Z}_n^*$)

$$= m^{1+k\cdot\varphi(n)} \pmod n$$

$$= m \cdot (m^{\varphi(n)})^k \pmod n$$

$$= m \cdot 1^k \pmod n$$

$$= m$$

Somit kann man mittels $c = m^x \bmod n$ verschlüsseln und mittels $c^{x'} \bmod n$ entschlüsseln.

Der Ver-/Entschlüsselungsschlüssel ist x bzw x'.

→ Pohlig-Hellman-Chiffrierung (hierbei n Primzahl, $\varphi(n) = n-1$)

Bemerkung: Die Berechnung des multiplikativen Inversen x' von x lässt sich effizient durchführen (später: erweiterter Euklid-Algorithmus)

Aufgabe: Berechne $5^{102} \bmod 101$!

Antwort: 101 ist eine Primzahl. Daher ist nach dem kleinen Satz von Fermat: $5^{100} \equiv 1 \pmod{101}$

Also ist $5^{101} = 5$ und $5^{102} = 25 \pmod{101}$.

Aufgabe: Berechne $\varphi(2^3 \cdot 5^4 \cdot 7 \cdot 11^2)$!

Antwort: $1 \cdot 2^2 \cdot 4 \cdot 5^3 \cdot 6 \cdot 10 \cdot 11^1$.

Aufgabe: Gegeben ist die zyklische Gruppe $\mathbb{Z}_n^*$ mit einem erzeugenden Element (auch Primitivwurzel genannt) a. Also: $\mathbb{Z}_n^* = \{a^1, a^2, \ldots, \underbrace{a^{\varphi(n)}}_{=1=a^0}\}$.

Gegeben sei ein Element b der Gruppe als Potenz von a: $b = a^i$.
Wie kann man feststellen, ob b eine Quadratzahl ist (sog. quadratischer Rest) und wenn ja, wie kann man eine Quadratwurzel von b bestimmen?
Antwort: b ist Quadratzahl, wenn i gerade ist.
Dann ist $a^{i/2}$ die Quadratwurzel.

Aufgabe: Mit dem kleinen Satz von Fermat gilt für alle Primzahlen n und $a \in \mathbb{Z}_n^*$, dass $a^{n-1} \equiv 1 \pmod{n}$. Kann man diese Tatsache ausnutzen, um zumindest im Fall n Primzahl leicht multiplikative Inverse von $a \in \mathbb{Z}_n^*$ auszurechnen? (Hinweis: $a^{n-1} = a \cdot a^{n-2}$)

Antwort: Aus dem Hinweis ergibt sich, dass a^{n-2} invers zu a ist. Man kann Inverse also durch eine modulare Exponentiation berechnen.

Aufgabe: Es soll a^n berechnet werden, wobei n eine Zweierpotenz ist (z.B. $n=16$)
Wie kann man mit relativ wenigen Rechenoperationen a^n berechnen?

Antwort: Durch fortgesetztes Quadrieren. Also falls $n=2^k$, so berechne $(\dots((a^2)^2)^2\dots)^2$ (k-mal).

Dies erfordert k Multiplikationen.

Die ersten Protokolle der Modernen Kryptographie

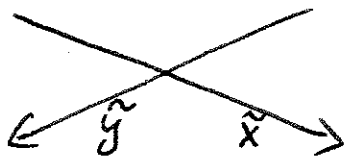
(noch vor den Public Key Systemen)

Diffie-Hellman-Schlüsselvereinbarung

Idee: Teilnehmer A und B vereinbaren durch wechselseitigen Nachrichtenaustausch einen geheimen Schlüssel z, der nach der Kommunikation A und B bekannt ist, und der anschließend für einen geheimen Nachrichtenaustausch zwischen A und B im Sinne der klassischen Kryptographie verwendet werden kann. Niemand, der die Kommunikation zwischen A und B abgehört hat, kann auf den Schlüssel z schließen.

Initialisierung: Man benötigt eine öffentlich bekannte große Primzahl n und eine Primitivwurzel a modulo n (also einen Erzeuger der Gruppe $\mathbb{Z}_n^*$).

Diffie-Hellman-Protokoll (Schlüsselvereinbarung)

Alice	Bob
Wählt Zufallszahl $x < n$	Wählt Zufallszahl $y < n$
Berechnet $\tilde{x} = a^x \bmod n$	Berechnet $\tilde{y} = a^y \bmod n$
	
Berechnet $z = (\tilde{y})^x \bmod n$ $= a^{xy} \bmod n$	Berechnet $z = (\tilde{x})^y \bmod n$ $= a^{xy} \bmod n$

Das Protokoll kann gebrochen werden, wenn der Diskrete Logarithmus $\tilde{x} \longmapsto x$ bzw. $\tilde{y} \longmapsto y$ berechnet werden kann.

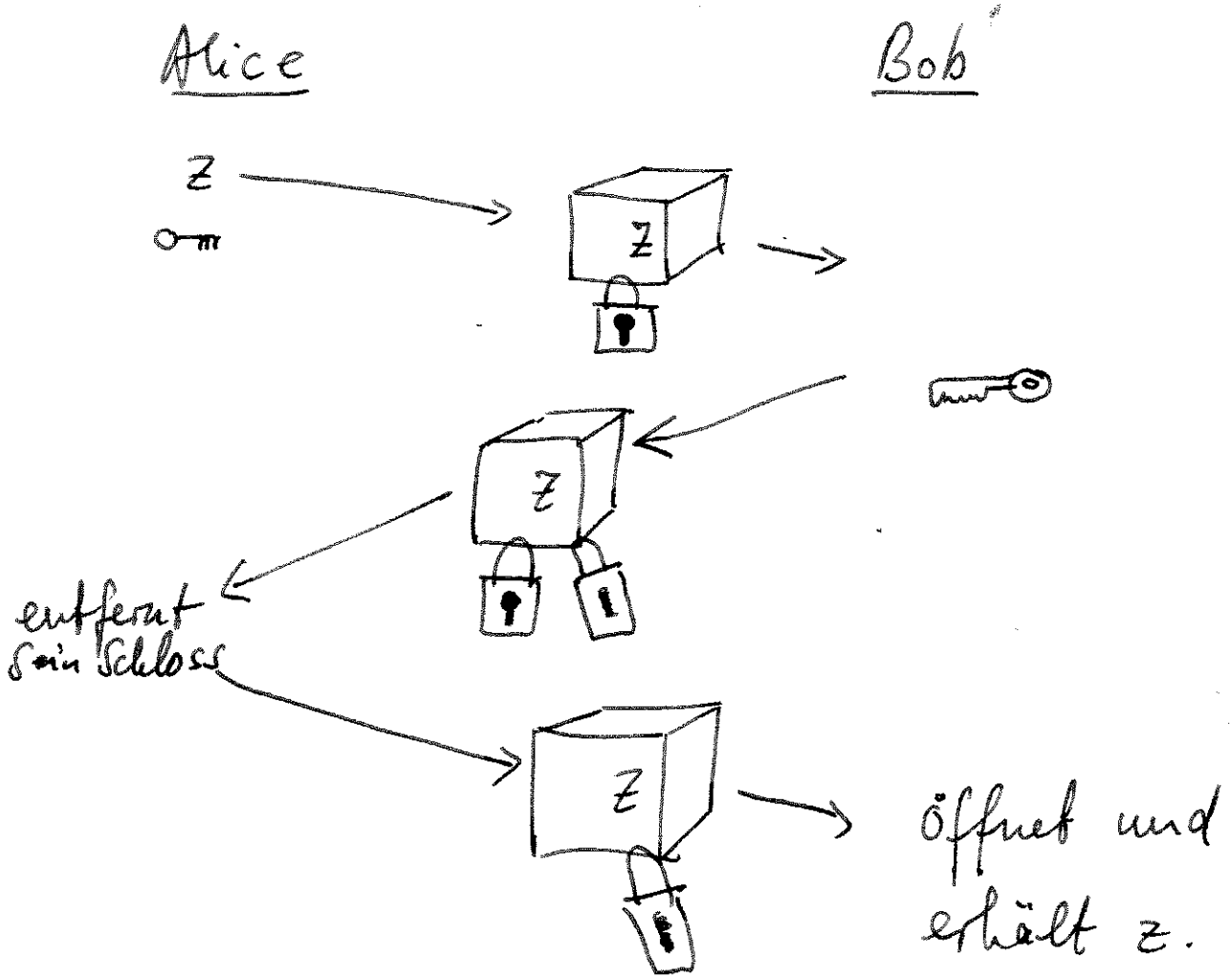
Die eigentliche zu lösende Aufgabe für einen Kryptoanalytiker ist das <u>Diffie-Hellman-Problem</u>:

<u>gegeben</u>: $(\tilde{x}, \tilde{y}) \longmapsto$ <u>finde</u> $z = a^{xy} \bmod n$

sowie n und a

No Key-Protokoll (oder 3-Runden-Protokoll) von Shamir: Es geht um den Austausch eines Schlüssels, den zunächst nur A besitzt. (evtl. die ganze Nachricht)

Idee: A, B besitzen individuelle Schlüssel, um ein Schloss, das sie an eine Box anbringen können, zu verschließen bzw. zu öffnen.



Alice	Bob
Besitzt Schlüssel z	
Berechnet $c = z^a \bmod n$	
$\xrightarrow{c}$	Berechnet $c^b \bmod n = d$
$\xleftarrow{d}$	
Berechnet $d^{a'} \bmod n = e$	
$\xrightarrow{e}$	Berechnet $e^{b'} \bmod n = z$

Hierbei ist n eine Primzahl, initial festgelegt.

Die Teilnehmer A, B haben initial a, a' bzw. b, b' so gewählt, dass $a \cdot a' \equiv 1 \pmod{n-1}$

$b \cdot b' \equiv 1 \pmod{n-1}$

Nachrechnen:

$$\underbrace{\underbrace{\underbrace{(z^a)}_{c}{}^b}_{d}{}^{a'}}_{e}{}^{b'} \equiv (z^{a \cdot a'})^{b \cdot b'}$$

$$\equiv z^{a a'}$$

$$\equiv z \pmod{n}$$

Shamir's No key-Protokoll kann gebrochen werden, sofern man Diskrete Logarithmen berechnen kann.

Shamirs Protokoll verwendet die (zuvor erwähnte) Pohlig-Hellman-Chiffrierung.
Diese ist kommutativ