Proseminar

Moderne Verfahren der Kryptographie

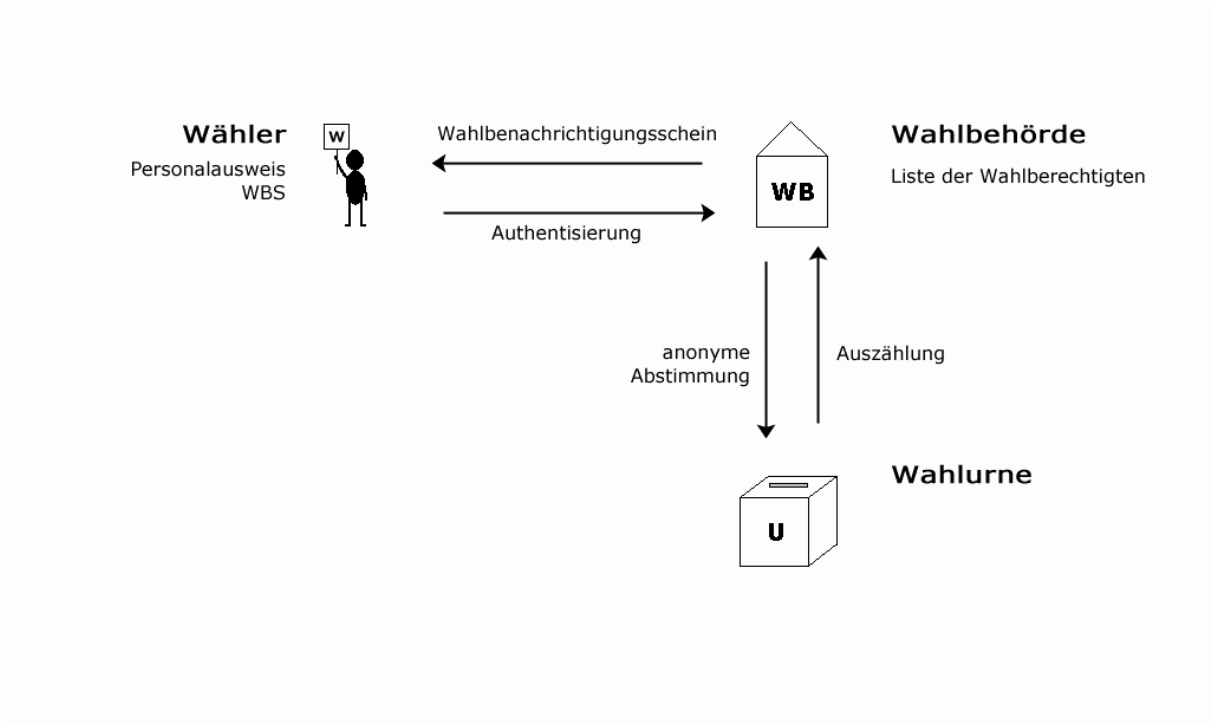
„**Elektronische Wahlen**“

1. Traditionelle Wahlen
2. Theoretischer Ansatz
3. Praktischer Ansatz

Elektronische Wahlen sind aufgrund der gegebenen technischen Möglichkeiten, die uns das Internet bietet, wieder in die Diskussion geraten. Dabei liegen die Vorteile der elektronischen Wahl klar auf der Hand:
Der Staat hat eine Kostenersparnis, da keine teilweise farbigen Wahlzettel mehr gedruckt werden müssen und die Anzahl der Wahlhelfer reduziert werden kann. Desweiteren ist von einer Zeitersparnis bei der Stimmabgabe (der Wähler muß das Haus nicht verlassen) und bei der Auszählung der abgegebenen Stimmen auszugehen. Der Wähler hat den Vorteil von jedem Ort aus wählen zu können. All diese Vorteile machen die elektronische Wahl schneller, kostengünstiger und flexibler und bilden damit die Voraussetzung für eine direktere Demokratie mit einer stärkeren Beteiligung der Bürger an wichtigen Entscheidungen.

Bevor diese Vorteile zum Tragen kommen, gilt es, eine sichere und stabile Wahlinfrastruktur aufzubauen. Dazu gehört ein Wahlprotokoll, das den Wahlvorgang zwischen Wähler und Wahlbehörde regelt, auf das ich in meinem Vortrag eingehen werde.

1. **Traditionelle Wahlen**

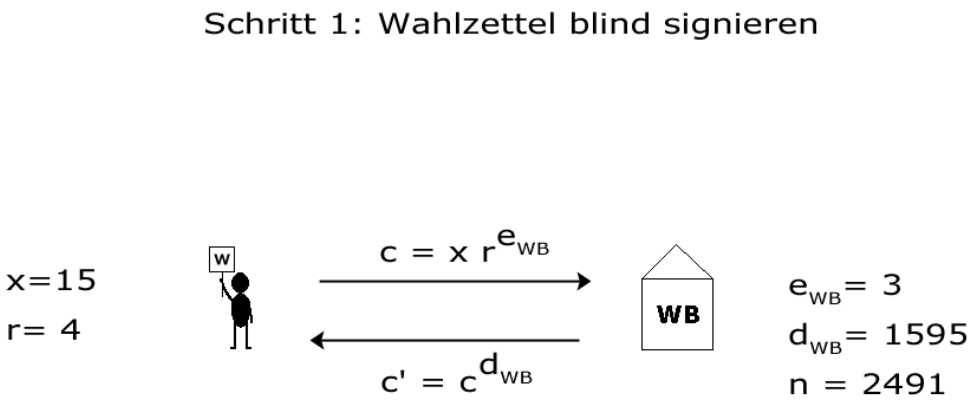


Heutige, in der Bundesrepublik anzutreffende Wahlen lassen sich meist in vier Phasen einteilen:
In der ersten Phase erstellt die Wahlbehörde eine Liste der Wahlberechtigten und informiert diese auf dem Postweg mit dem Wahlbenachrichtigungsschein.
In der zweiten Phase erscheint der Wähler in der Wahlbehörde und authentisiert sich mit seinem Personalausweis/Paß als Wahlberechtigter. Er erhält die Wahlunterlagen.
Die dritte Phase ist gekennzeichnet durch die anonyme Stimmabgabe, das heißt durch das geheime Setzen eines Kreuzes auf die Wahlunterlagen und die Durchmischung der Wahlunterlagen in der Wahlurne.
Die Auszählung der Stimmen und Bekanntgabe des Ergebnisses erfolgt in der letzten Phase.

2. Theoretischer Ansatz

Annahmen: Die Wahlbehörde sorgt dafür, daß nur die Wahlberechtigten einen und nur einen Wahlzettel erhalten.

Schritt 1: Wahlzettel blind signieren



Voraussetzung: Der Wahlzettel(x) hat eine von der Wahlbehörde(WB) vorgegebene Struktur (z.B: Palindrom oder nur bestimmte Ziffern).

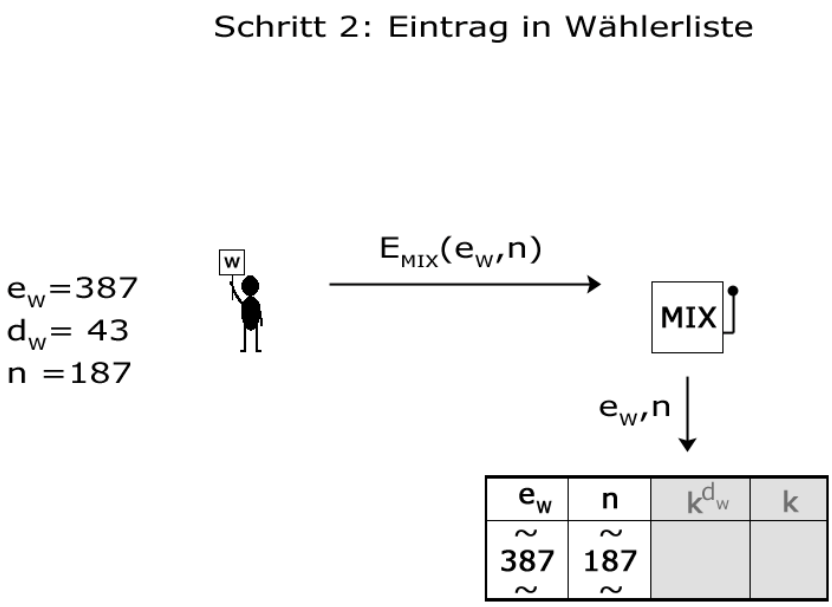
Der Wähler(W) will seinen Wahlzettel(x) von der Wahlbehörde(WB) blind signieren lassen. Das heißt WB darf den Inhalt von x nicht erfahren. Dazu denkt sich W eine Zufallszahl(r) aus und verschlüsselt sie mit dem öffentlichen Schlüssel von WB. Das Resultat multipliziert er mit x und schickt es an WB. WB wendet seinen privaten Schlüssel darauf an und schickt das Ergebnis zurück an W. Das muß nun W durch seine Zufallszahl dividieren und erhält x mit der Signatur von WB.

Beispiel:
$e_{WB}=3$
$d_{WB}=1595$
$x=15$
$r=4$

$c = x*r^{\mathbf{e}_{WB}} = 15*4^{\mathbf{3}} \bmod 2491 = 960$
$c` = c^{\mathbf{d}_{WB}} = 960^{\mathbf{1595}} \bmod 2491 = 1548$
$z = c` / r = 387 = x^{\mathbf{d}_{WB}} = e_W$

RSA-Schlüsselgenerierung für WB
$n=pq$
$2491=47*53$
$\phi(n)=(p-1)*(q-1)=2392$
$e*d=\phi(n)*k+1$
$3*d=2392*k+1$
$k=2$
$d=1595$

Schritt 2: Eintrag in Wählerliste



Voraussetzung: $e_W=x^{d_{WB}}=387$ ist der öffentliche Schlüssel des Wählers.
Dazu muß er sich noch einen privaten Schlüssel berechnen.

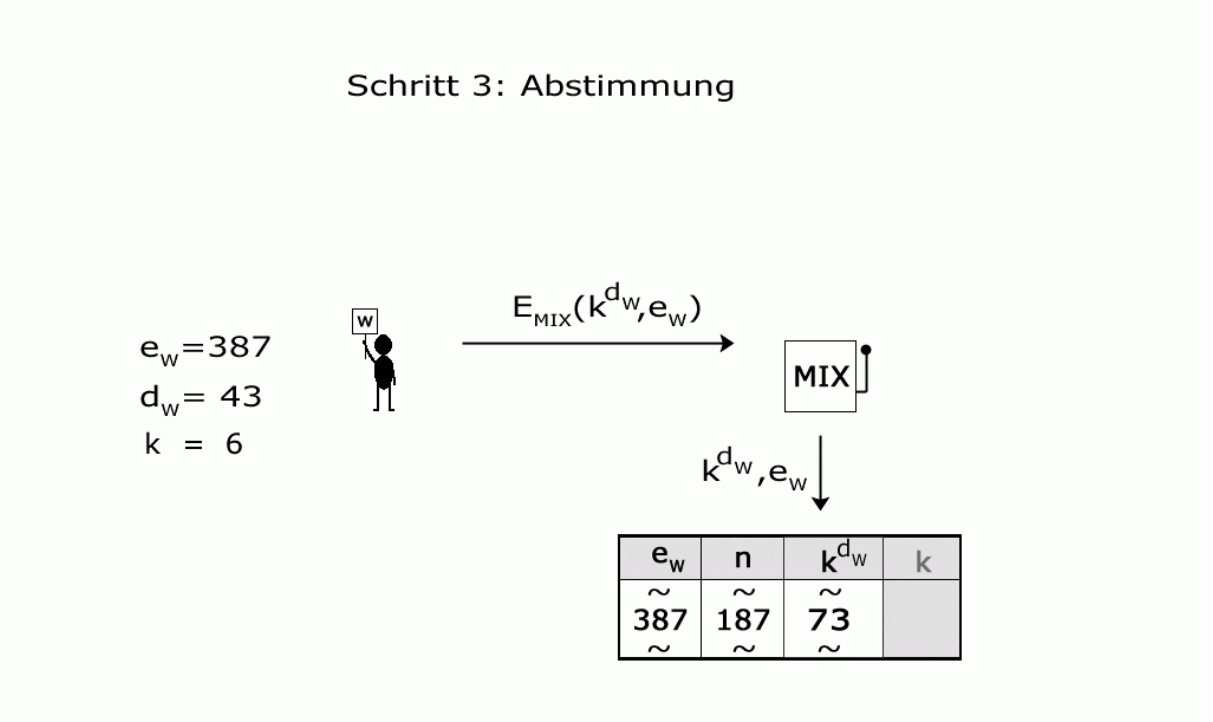
Beispiel:
eW=387
dW=43
n=187

Der Wähler läßt nun seinen öffentlichen Schlüssel e_W und das Primzahlenprodukt n über einen MIX in die Wählerliste eintragen. Damit ist die Wahlbehörde nicht in der Lage, den Eigentümer des öffentlichen Schlüssels zu ermitteln.

EMIX(e_W, n) = EMIX(387, 187)

RSA-Schlüsselgenerierung für WB
n=pq
187=17*11
ϕ(n)=(p-1)*(q-1)=160
e*d=ϕ(n)*k+1
387*d=160*k+1
k=104
d=43

Schritt 3: Abstimmung

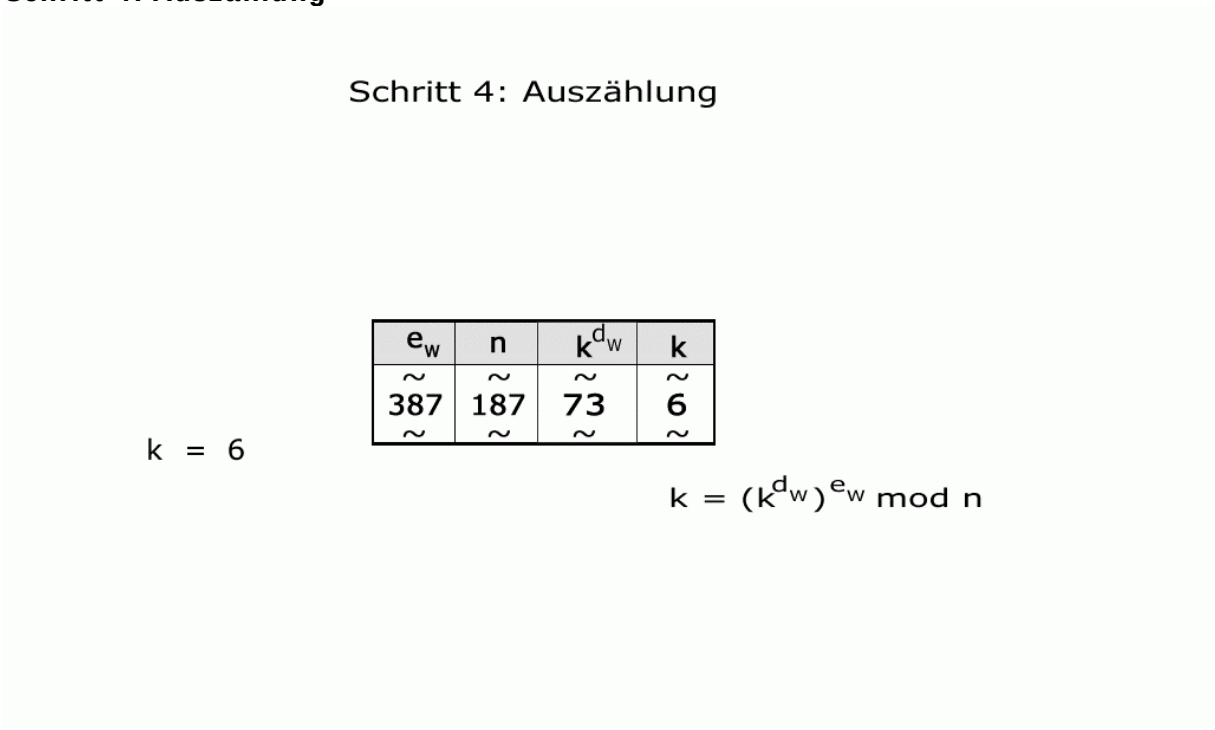


Der Wähler stimmt für seine Partei indem er eine der Partei zugeordnete Ziffer(k) mit seinem privaten Schlüssel signiert und wieder über einen MIX in die Wählerliste eintragen läßt.

Beispiel:
$e_w = 387$
$d_w = 43$
$k = 6$
$k^{d_w} = 6^{43} \bmod 187 = 73$

$EMIX(k^{d_w}, e_w) = EMIX(73, 387)$

Schritt 4: Auszählung



Der Wahlvorgang ist abgeschlossen. Die Wählerliste wird vom Wahlleiter ausgezählt. Dazu wird auf jede signierte Stimme der dazugehörige öffentliche Schlüssel e_W angewendet und die Stimme erscheint im Klartext.

Beispiel:
$e_W = 387$
$n = 187$
$k^{d_W} = 73$

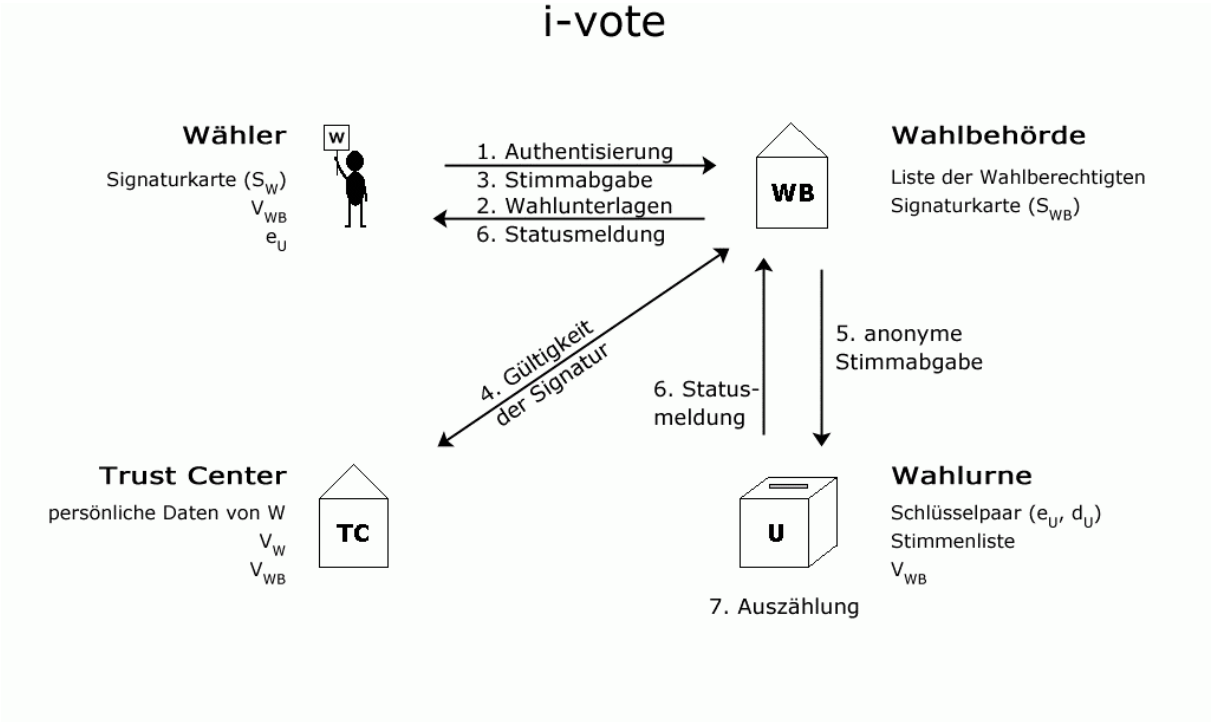
$k = (k^{\mathbf{d}_W})^{\mathbf{e}_W} \bmod n = 73^{\mathbf{387}} \bmod 187 = 6$

Kontrolle:
Um sicherzustellen, daß alle in der Wählerliste eingetragenen öffentlichen Schlüssel auch gültige Wahlzettel sind, muß man nur auf die öffentlichen Schlüssel der Wähler den Verifikationsschlüssel der Wahlbehörde anwenden und prüfen, ob das Resultat (= x) die von der Wahlbehörde vorgegebene Struktur aufweist (Palindrom, bestimmte Ziffern).
Um sicherzustellen, daß jeder nur eine Stimme abgegeben hat, muß man nur die Wählerliste dahingehend überprüfen, ob jedem Wahlzettel $x^{\mathbf{d}_{WB}}$ (= e_W) höchstens eine Stimme zugeordnet ist.

3. Praktischer Ansatz

In zahlreichen praktischen Versuchen hat sich das Wahlprotokoll i-vote der Forschungsgruppe Internetwahlen der Universität Osnabrück, das vom Bundesministerium für Wirtschaft gefördert wird, bewährt. Immer wurde es als zusätzliches Wahlverfahren neben den traditionellen angeboten, so z.B. bei
der simulierten Bundestagswahl mit dem Titel „Wahlkreis 329“
der Sozialwahl 1999 bei der TKK Hamburg
der Jugendgemeinderatswahl 2001 in Esslingen
der Studentenparlamentswahl 2001 der Universität Osnabrück
der simulierten Personalratswahl 2001 in Brandenburg
der Wahl des akademischen Senats 2001 der Hochschule Bremerhaven.

Voraussetzung für den Wähler sind eine digitale Signatur auf einer Chipkarte, ein Chipkarten-Lesegerät und ein Computer mit Internetzugang.



Die Wahl erfolgt in sieben Phasen.

1. Der Wähler authentisiert sich gegenüber der Wahlbehörde mit seinen persönlichen Daten und der Signaturkarte, woraufhin die Wahlbehörde prüft, ob der Wähler bereits seine Stimme abgegeben hat.

2. Die Wahlbehörde schickt die Wahlunterlagen (Applet mit signiertem Wahlzettel) an den Wähler.

3. Anhand der Signatur des Wahlzettels kann der Wähler prüfen, ob tatsächlich die Wahlbehörde der Absender ist. Der Wähler macht darauf sein Kreuz und verschlüsselt seine Stimme mit dem öffentlichen Schlüssel der Wahlurne und schickt sie signiert und unsigniert zurück an die Wahlbehörde.

4. Die Wahlbehörde prüft die Gültigkeit der Signatur des Wählers beim Trust-Center, indem persönliche Daten und Signatur verglichen werden. Den vom Trust-Center erhaltenen Verifikationsschlüssel wendet die Wahlbehörde auf die vom Wähler signierte Stimme an und prüft die Übereinstimmung mit der unsignierten Stimme. Damit ist sichergestellt, daß der Wähler der ist, für den er sich ausgibt.

5. Die vom Wähler verschlüsselte, unsignierte Stimme wird von der Wahlbehörde signiert und an die Wahlurne weitergeleitet. Somit weiß die Wahlurne nicht, von wem die Stimme stammt.

6. Die Stimme wird vorerst nur gespeichert, bis die Wahlzeit vorüber ist. Die Wahlurne schickt eine Statusmeldung an die Wahlbehörde und die Wahlbehörde schickt sie an den Wähler. Der Wahlvorgang ist abgeschlossen.

7. Es erfolgt die Auszählung der Stimmen. Dazu wird auf jede Stimme der Verifikationsschlüssel der Wahlbehörde angewandt, um die Wahlbehörde als Absender zu identifizieren. Dann wird mit dem privaten Schlüssel der Wahlurne die verschlüsselte Stimme des Wählers entschlüsselt.

Das Verfahren ist nur so sicher wie das RSA-Verfahren, da die digitale Signatur und das Schlüsselpaar der Wahlurne auf dem RSA-Algorithmus basieren.
Die sichere Authentisierung wird mittels der digitalen Signatur gewährleistet und die Anonymität durch die physikalische und logische Trennung von Wahlbehörde und Wahlurne.

Das Wahlverfahren ist schon ziemlich weit ausgereift, aber noch nicht „serienreif“, da sich bei den Testwahlen Probleme gezeigt haben, die erst beseitigt werden müssen. So funktioniert das Verfahren zur Zeit nur mit dem Internet Explorer. Die Treiber für das Lesegerät sind auch noch nicht ganz ausgereift und einen Internet-Zugang hat noch nicht jeder.
Für die Zukunft ist angedacht, die Sozialwahl 2004 kostensparend online abzuwickeln und wenn sie erfolgreich verläuft, dann vielleicht auch die Bundestagswahl 2006.