

BAYERISCHE AKADEMIE DER WISSENSCHAFTEN
MATHEMATISCH-NATURWISSENSCHAFTLICHE KLASSE

ABHANDLUNGEN · NEUE FOLGE, HEFT 176

Friedrich L. Bauer

Die Komödie der Irrungen
im Wettstreit der Kryptologen

Vorgetragen in der Sitzung
vom 14. Dezember 2007

MÜNCHEN 2008

VERLAG DER BAYERISCHEN AKADEMIE DER WISSENSCHAFTEN
IN KOMMISSION BEIM VERLAG C. H. BECK MÜNCHEN

Inhalt

A COMEDY OF ERRORS	4
Charakterisierung der Irrungen	5
SYSTEMBEDINGTE EINBRUCHSMÖGLICHKEITEN	6
Fehler durch Bequemlichkeit und Materialeinsparung	6
Die Tücke der <i>complication illusoire</i>	6
Perfekte Sicherheit und praktische Sicherheit	11
Fehlerhafte Chiffriervorschriften	11
CHIFFRIERFEHLER DURCH LEICHTSINN ODER FAULHEIT DER BENUTZER ..	13
1. Das Chiffriersystem wird durch den zum Geheimtext gehörigen Klartext (oder einen Teil davon) kompromittiert (Klartext-Geheimtext-Kompromittierung)	13
2. Das Chiffriersystem wird durch die Übertragung der Chiffrate ein und des selben Klartextes mit zwei verschiedenen Schlüsseln kompromittiert (Geheimtext-Geheimtext-Kompromittierung)	14
3. Das Chiffriersystem wird durch die Übertragung der Chiffrate zweier verschiedener Klartexte mit ein und dem selben Schlüssel kompromittiert (Klartext-Klartext-Kompromittierung)	14
NOCHMALS: SYSTEMBEDINGTE EINBRUCHSMÖGLICHKEITEN	16
Ironie des Schicksals: Unterschätzung des Gegners	16
Geheimhaltung und Authentizität im Konflikt	16
CHIFFRIERFEHLER NOCH UND NOCH	17
Mangelnde Überwachung und andere Überheblichkeiten führen zum Ruin	17
NOCHMALS: DIE KOMÖDIE DER IRRUNGEN	19