WHY WE NEED CRYPTOGRAPHY

The only known practical means of protecting data in a communications network.

System security tool for online banking, payments e-commerce and m-commerce to achieve:

a) confidentiality
b) integrity
c) authentication
d) digital signature
LARGEST KNOWN DATA BREACH CONSPIRACY
160 million credit cards hacked (2005 – 2012)

- Global Payment Systems
- Heartland Payment Systems
- Visa Jordan / Commidea / Dexia Bank
- Wet Seal / 7-Eleven / JetBlue Airways
- JC Penney / Carrefour / Hannaford
- Euronet / Dow Jones / Nasdaq
- Diners Singapore / Ingenicard
160 MILLION
CREDIT CARD NUMBERS

7-year hacking scheme the 'cutting edge' of financial fraud

UNITED STATES OF AMERICA
CREDIT CARD
$10
1234 5678 9876 5432

CANADA
CREDIT CARD
$15
1234 5678 9876 5432

EUROPEAN UNION
CREDIT CARD
$50
1234 5678 9876 5432
ATM skimming fraud is costing the US banking industry about $1 billion each year.

“Attacks on payments systems have exploded in the past two years” said the US Secret Service.

According to the US Secret Service, payment card fraud in America is at least $8 billion annually.

According to the National Retail Federation, credit card fraud exceeded $11 billion in 2012.
HOW MASSIVE IS PAYMENT CARD FRAUD?

What is the role of cryptographic security?
WHAT IS CRYPTOGRAPHY?

Encryption and decryption

Permutation, substitution = product cipher

Symmetric cipher: same secret key to encrypt, decrypt

Asymmetric cipher: public key, private key
<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Key Length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Weak</td>
</tr>
<tr>
<td>DES</td>
<td>56</td>
</tr>
<tr>
<td>RC4 SSL</td>
<td>40</td>
</tr>
<tr>
<td>RSA</td>
<td>768</td>
</tr>
<tr>
<td>ECC</td>
<td>136</td>
</tr>
<tr>
<td>MD5</td>
<td></td>
</tr>
<tr>
<td>SHA256</td>
<td></td>
</tr>
<tr>
<td>AES</td>
<td></td>
</tr>
</tbody>
</table>
ENCRYPTION ALGORITHM – 3DES

Key size: 168 bits
ENCRYPTION ALGORITHM – AES

Algorithm:
- DES
- Triple DES
- AES 256
- SHA256

Key: 1234567890ABCDEF1234567890ABCDEF1234567890ABCDEF

Message: This is a test message.

Encrypted message: 65d425aacb2b09b65eb25f88476a318f35974920a9a0fb8deb3bde76c1f5dae

Decrypted message: This is a test message.
HASHING ALGORITHM – SHA256

Algorithm:
- DES
- Triple DES
- AES
- SHA256

Key: NA

Message: This is a test message.

Hashed message: 0668b515bfc41b90b6a90a6ae8600256e1c76a67d17c78a26127ddeb9b324435

Decrypted message: NA
eBANKING & ATM/POS SYSTEMS

- PSTN / WIFI
- INTERNET
- Web Server
- IVR / Biometrics
- ATM / EFTPOS
- Cards / M-Apps
- Authentication
- Verification
- Authorisation
- Core Banking System
ONLINE BANKING SECURITY ARCHITECTURE

- HOST
- ONLINE BANKING SECURITY ARCHITECTURE
- Crypto Server
- IPS Sensor
- APPLET
- SECURE SOCKETS LAYER (SSL) + APPLICATION LAYER END TO END ENCRYPTION
- Firewall
- OTP verification
- AVS
- Web Server
- Database Server
- Application Server
- Customer ID PIN (encrypted)
- 4 types of OTP with Transaction Alerts
- HSM
- Cryptographic functions
Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

* Refer to the certification authority's statement for details.

**Issued to:** internet-banking.dbs.com.sg

**Issued by:** VeriSign Class 3 Extended Validation SSL SGC CA

**Valid from:** 05-12-13 to 10-01-15

**Show:** <All>

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>V3</td>
</tr>
<tr>
<td>Serial number</td>
<td>46 ea e4 81 a2 39 8...</td>
</tr>
<tr>
<td>Signature algorithm</td>
<td>sha1RSA</td>
</tr>
<tr>
<td>Signature hash alg...</td>
<td>sha1</td>
</tr>
<tr>
<td>Issuer</td>
<td>VeriSign Class 3 Extended Validation SSL</td>
</tr>
<tr>
<td></td>
<td>SGC CA</td>
</tr>
<tr>
<td>Valid from</td>
<td>Thursday, 05 December 2013</td>
</tr>
<tr>
<td>Valid to</td>
<td>Saturday, 10 January 2014</td>
</tr>
<tr>
<td>Subject</td>
<td>internet-banking.db...</td>
</tr>
<tr>
<td>Public key</td>
<td>RSA (2048 Bits)</td>
</tr>
<tr>
<td>Subject Alternative...</td>
<td>DNS Name=internet-banking.db...</td>
</tr>
<tr>
<td>Basic Constraints</td>
<td>Subject Type=End</td>
</tr>
<tr>
<td>Enhanced Key Usage</td>
<td>Server Authentication</td>
</tr>
<tr>
<td>Subject Key Ident...</td>
<td>0a aa 2b fd 83 1c 6...</td>
</tr>
<tr>
<td>Authority Key Ident...</td>
<td>KeyID=4e 43 c8 1d ...</td>
</tr>
<tr>
<td>CRL Distribution P...</td>
<td>[1]CRL Distribution ...</td>
</tr>
</tbody>
</table>
PIN MECHANICS

A/C #

KEY

DES

Chosen PIN

Derived PIN

PIN OFFSET

908679 → 203011 = 705668
HSM calculates new Derived PIN from A/C # then adds it to previously stored PIN OFFSET for comparison with Chosen PIN.
ATM NETWORKS

SHARED LOCAL NETWORK: >2,000 ATMs in Singapore

Global Networks:

VISA | PLUS | MasterCard | Cirrus

State Bank of India
ATM5 NETWORK

ATMs at 153 locations

- Citibank
- Standard Chartered
- HSBC
- Maybank
- ANZ
- State Bank of India

CIRRUS

- eKH(PIN)
- eKC(PIN)
- eKM(PIN)
KEY EXCHANGE
**KEY EXCHANGE PERMUTATION**

Number of keys: \( n(n-1)/2 = 6(6-1)/2 = 15 \)

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>C</td>
<td>D</td>
<td>E</td>
<td>F</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>D</td>
<td>E</td>
<td>F</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D</td>
<td>E</td>
<td>F</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E</td>
<td>F</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td></td>
<td>15</td>
</tr>
</tbody>
</table>

Total
DES KEY MANAGEMENT

Key generation
Key distribution
Key installation
Key recovery

Master keys
Key encrypting keys
Data encrypting keys
KEY MANAGEMENT

\[ \text{KT}_1 \quad \text{KT}_2 \quad \text{KT}_n \]

\[ \text{eKM(KDE1)} \\
\text{eKM(KDE2)} \\
\text{eKM(KDEn)} \]

\[ \text{SCM} \\
\text{KM} \]
RANDOM # = eKMO(KDE)
EN[eKMO(KDE), PIN] = eKDE(PIN)
DE[eKMO(KDE), eKDE(PIN)] = PIN (disallowed)
VE[eKMO(KDE), eKDE(PIN_i), eKM2(PIN_v)]
$45 MILLION ATM HEISTS

RAKBANK CYBERATTACK
DECEMBER 22, 2012 @ 2:40PM - 5:05PM
36,000+ TRANSACTIONS | 20 COUNTRIES | $5 MILLION IN LOSS

BANK OF MUSCAT CYBERATTACK
FEBRUARY 19, 2013 @ 3:00PM - FEBRUARY 20, 2013 @ 1:26AM
40,500+ TRANSACTIONS | 27 COUNTRIES | $45 MILLION IN LOSS
Note: acquiring bank layer is not shown

$5M

$40M

MasterCard
BANKNET

Cirrus

ecs
an Opus company

enStage
ANATOMY OF A MAGNETIC STRIPE

<table>
<thead>
<tr>
<th>Start</th>
<th>Card Number</th>
<th>Separator</th>
<th>Expiry Date</th>
<th>Service Code</th>
<th>Discretionary</th>
<th>End</th>
</tr>
</thead>
</table>

; nnnn nnnn nnnn nnnn = YYMM SVC DDDDDDDD[CVV] X

THE ACHILLES HEEL OF PAYMENT CARD SECURITY
CHIP AND MAGNETIC STRIPE

Card Number  Expiry Date  Service Code  Discretionary  CVC

THE ACHILLES HEEL OF PAYMENT CARD SECURITY
CARD DATA AND PERSONAL DETAILS OF 110 MILLION CUSTOMERS WERE HACKED BETWEEN 27 NOV AND 15 DEC 2013.
INFORMATION ON 70 MILLION TAKEN IN TARGET DATA BREACH

WASHINGTON POST JANUARY 11, 2014 - Target said Friday that the thieves who stole massive amounts of credit and debit card information during the holiday season also swept up names, addresses, and phone numbers of 70 million customers, information that could put victims at greater risk for identity theft.
Can hackers decrypt Target's PIN data?

**ENCRYPTION FORMAT IN ECB MODE**

1. XOR PIN AND PAN
2. CONCATENATE PIN AND TRANSACTION NUMBER
3. PAD PIN WITH RANDOM VALUE
4. PAD PIN WITH FIXED VALUE
(PIN) 0x1234FF0000000000 ⊕ (PAN) 0x937492492032 = 0x81406DB6DFCD

(PIN) 0x1234FF0000000000 ⊕ (PAN) 0x274965382343 = 0x357D9AC7DCBC
PAYMENT CARD FRAUD

WHAT DO WE KNOW?
HOW MUCH DO WE KNOW?
## Payment Card and Online Banking Security Enhancement Roadmap

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1Q</td>
<td>2Q</td>
<td>3Q</td>
<td>4Q</td>
<td>1Q</td>
</tr>
<tr>
<td>DDA Credit/Debit Chip Card Migration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>D</td>
</tr>
<tr>
<td>DDA ATM Chip Card Migration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>One Time Password for Card Not Present</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>D</td>
</tr>
<tr>
<td>New/Replacement Card Activation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cessation of Domestic Magstripe Transactions for Credit/Debit Card</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transaction Alerts</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deactivation of Overseas Cash Withdrawal for ATM Card</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transaction Signing for Online Banking</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deactivation of Overseas Use of Magstripe for Credit/Debit/Prepaid Card</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**DDA**: Dynamic Data Authentication  
**ATM**: Automated Teller Machine
ONLINE BANKING SECURITY ARCHITECTURE

- Security Server
- IPS Sensor
- APPLET
- OTP & Biometrics
- Firewall
- SSL
- APPLICATION LAYER END TO END ENCRYPTION
- AVS
- Configuration Management Controls
- HSM
- Cryptographic functions

Transaction Signing (1 January 2013)

- Web Server
- Application Server
- Database Server

BIOMETRICS

- IRIS
- VOICE
- FACE
- FINGERPRINT
- VEIN
BIOMETRICS
AUTHENTICATION

• WHAT YOU KNOW

• WHAT YOU HAVE

• WHO YOU ARE

(BIOMETRICS)

The automatic identification or identity verification of living persons based on behavioural and physiological characteristics.
BIOMETRICS

A general term to describe a process or a characteristic.

1. Automated methods of recognizing a person based on measurable behavioural and physiological characteristics.

2. A measurable physiological and behavioural trait that can be used for automated recognition.
SURVEY 2012
80 BANKS
Australia
Belgium
Brazil
Brunei
Canada
Chile
China
Germany
Indonesia
Ireland
Israel
Italy
Japan
Jordan
Pakistan
Poland
Mexico
Panama
Russia
Spain
Turkey
UAE
UK
USA
<table>
<thead>
<tr>
<th>Bank</th>
<th>Country</th>
<th>Verification Method</th>
<th>Access Method</th>
<th>Column</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANZ BANK</td>
<td>AUSTRALIA</td>
<td>VOICE</td>
<td>TELEPHONE</td>
<td>1</td>
</tr>
<tr>
<td>ST GEORGE BANK</td>
<td>AUSTRALIA</td>
<td>VOICE</td>
<td>TELEPHONE</td>
<td>2</td>
</tr>
<tr>
<td>NATIONAL AUSTRALIA BANK</td>
<td>AUSTRALIA</td>
<td>VOICE</td>
<td>TELEPHONE</td>
<td>3</td>
</tr>
<tr>
<td>DEXIA PRIVATE BANK</td>
<td>BELGIUM</td>
<td>VOICE</td>
<td>TELEPHONE</td>
<td>4</td>
</tr>
<tr>
<td>TD WATERHOUSE</td>
<td>CANADA</td>
<td>VOICE</td>
<td>TELEPHONE</td>
<td>5</td>
</tr>
<tr>
<td>CHINA MERCHANT BANK</td>
<td>CHINA</td>
<td>VOICE</td>
<td>TELEPHONE</td>
<td>6</td>
</tr>
<tr>
<td>FIRST DIRECT BANK</td>
<td>ISRAEL</td>
<td>VOICE</td>
<td>TELEPHONE</td>
<td>7</td>
</tr>
<tr>
<td>DISCOUNT BANK</td>
<td>ISRAEL</td>
<td>VOICE</td>
<td>TELEPHONE</td>
<td>8</td>
</tr>
<tr>
<td>BANK HAPOALIM</td>
<td>ISRAEL</td>
<td>VOICE</td>
<td>TELEPHONE</td>
<td>9</td>
</tr>
<tr>
<td>BARCLAYS</td>
<td>UK</td>
<td>VOICE</td>
<td>TELEPHONE</td>
<td>10</td>
</tr>
<tr>
<td>SOMER TRUST BANK</td>
<td>USA</td>
<td>VOICE</td>
<td>TELEPHONE</td>
<td>11</td>
</tr>
<tr>
<td>BANK OF AMERICA</td>
<td>USA</td>
<td>VOICE</td>
<td>TELEPHONE</td>
<td>12</td>
</tr>
<tr>
<td>LA CAIXA BANK</td>
<td>BRAZIL</td>
<td>FINGERPRINT</td>
<td>ATM</td>
<td>1</td>
</tr>
<tr>
<td>ITAUTEC BANK</td>
<td>BRAZIL</td>
<td>FINGERPRINT</td>
<td>ATM</td>
<td>2</td>
</tr>
<tr>
<td>BANK ISLAM BRUNEI</td>
<td>BRUNEI</td>
<td>FINGERPRINT</td>
<td>ATM</td>
<td>3</td>
</tr>
<tr>
<td>BANCAFE BANK</td>
<td>CHILE</td>
<td>FINGERPRINT</td>
<td>ATM</td>
<td>4</td>
</tr>
<tr>
<td>LETO BANK VTB</td>
<td>RUSSIA</td>
<td>FINGERPRINT</td>
<td>ATM</td>
<td>5</td>
</tr>
<tr>
<td>STANDARD BANK</td>
<td>SOUTH AFRICA</td>
<td>FINGERPRINT</td>
<td>ATM</td>
<td>6</td>
</tr>
<tr>
<td>BARCLAYS BANK</td>
<td>UAE</td>
<td>FINGERPRINT</td>
<td>ATM</td>
<td>7</td>
</tr>
<tr>
<td>Bank Name</td>
<td>Country</td>
<td>Authentication Method</td>
<td>ATM Type</td>
<td>Order</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>----------</td>
<td>-----------------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>JAPAN POST BANK</td>
<td>JAPAN</td>
<td>FINGERVEIN</td>
<td>ATM</td>
<td>1</td>
</tr>
<tr>
<td>SUMITOMO MITSUI</td>
<td>JAPAN</td>
<td>FINGERVEIN</td>
<td>ATM</td>
<td>2</td>
</tr>
<tr>
<td>MIZUHO BANK</td>
<td>JAPAN</td>
<td>FINGERVEIN</td>
<td>ATM</td>
<td>3</td>
</tr>
<tr>
<td>BANK OF TOKYO</td>
<td>JAPAN</td>
<td>FINGERVEIN</td>
<td>ATM</td>
<td>4</td>
</tr>
<tr>
<td>JUROKU BANK</td>
<td>JAPAN</td>
<td>FINGERVEIN</td>
<td>ATM</td>
<td>5</td>
</tr>
<tr>
<td>JOYO BANK</td>
<td>JAPAN</td>
<td>FINGERVEIN</td>
<td>ATM</td>
<td>6</td>
</tr>
<tr>
<td>TAJIMA BANK</td>
<td>JAPAN</td>
<td>FINGERVEIN</td>
<td>ATM</td>
<td>7</td>
</tr>
<tr>
<td>RESONA BANK</td>
<td>JAPAN</td>
<td>FINGERVEIN</td>
<td>ATM</td>
<td>8</td>
</tr>
<tr>
<td>BANK OF FUKUOEA</td>
<td>JAPAN</td>
<td>FINGERVEIN</td>
<td>ATM</td>
<td>9</td>
</tr>
<tr>
<td>CITIBANK</td>
<td>JAPAN</td>
<td>FINGERVEIN</td>
<td>ATM</td>
<td>10</td>
</tr>
<tr>
<td>BPH BANK</td>
<td>POLAND</td>
<td>FINGERVEIN</td>
<td>ATM</td>
<td>11</td>
</tr>
<tr>
<td>VAKIFBANK</td>
<td>TURKEY</td>
<td>FINGERVEIN</td>
<td>ATM</td>
<td>12</td>
</tr>
<tr>
<td>ISBANK</td>
<td>TURKEY</td>
<td>FINGERVEIN</td>
<td>ATM</td>
<td>13</td>
</tr>
<tr>
<td>BANCO BRADESCO</td>
<td>BRAZIL</td>
<td>HANDVEIN</td>
<td>ATM</td>
<td>1</td>
</tr>
<tr>
<td>TOKYO MITSUBISHI</td>
<td>JAPAN</td>
<td>HANDVEIN</td>
<td>ATM</td>
<td>2</td>
</tr>
<tr>
<td>OGAKI KYORITSU BANK</td>
<td>JAPAN</td>
<td>HANDVEIN</td>
<td>ATM</td>
<td>3</td>
</tr>
<tr>
<td>HIROSHIMA BANK</td>
<td>JAPAN</td>
<td>HANDVEIN</td>
<td>ATM</td>
<td>4</td>
</tr>
<tr>
<td>SURUGA BANK</td>
<td>JAPAN</td>
<td>HANDVEIN</td>
<td>ATM</td>
<td>5</td>
</tr>
<tr>
<td>NANTO BANK</td>
<td>JAPAN</td>
<td>HANDVEIN</td>
<td>ATM</td>
<td>6</td>
</tr>
<tr>
<td>ZIRAAT BANK</td>
<td>TURKEY</td>
<td>HANDVEIN</td>
<td>ATM</td>
<td>7</td>
</tr>
</tbody>
</table>
iPhone 5S Touch ID
Apple iPhone 5S Touch ID

- Laser-cut sapphire crystal
- Stainless steel detection ring
- Tactile switch
- Touch ID sensor
- FAR = 0.002%
VENDOR CLAIMS OF BIOMETRIC ACCURACY

FINGERPRINT / AuthenTec
• FAR 0.0002%
• FRR 1.0%

FINGER-VEIN / Hitachi-Omron
• FAR 0.0001%
• FRR 0.01%

PALM-VEIN / Fujitsu
• FAR 0.00008%
• FRR 0.01%
VOICE BIOMETRICS

Step 1: System: Please enter your account number using your touch-tone keypad
Caller: 235167

Step 2: System: Please say your password
Caller: Merry go round
System: Thank you.

(a) Text-dependent verification.

System: Please say your account number
Caller: 235167
System: Thank you.

(b) Text-dependent verification with speech recognition.
(c) Text-prompted verification.

Call Center Agent with caller ID: What can I do for you, Ms. Jones?
Caller: I want to transfer $100,000 from my savings account with you to an offshore account in Bimini that I have just opened.
Agent: Let me look into that. Please wait while I am getting the information.
PAUSE while the system is verifying the identity of the caller
Agent: Thank you for your patience. I will process that request now.

(d) Text-independent verification.
FAR Vs FRR

- More Secure
- More Convenient
- Higher Performance

False Reject Rate vs False Accept Rate (FAR)

Points: A, B, C
Figure 6. Detection error trade-off: Best of 3 attempts
BASIC COMPONENTS OF A BIOMETRIC SYSTEM

TOP FIVE THREATS TO BIOMETRICS

1. IMPERSONATION
2. CIRCUMVENTION
3. SUBSTITUTION
4. REPUDIATION
5. COERCION
finis